Internet y derechos humanos II

Aportes para la discusión en América Latina

Eduardo Bertoni
COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información





Internet y derechos humanos II

Aportes para la discusión en América Latina

Internet y derechos humanos II

Aportes para la discusión en América Latina

Eduardo Bertoni
COMPILADOR

Facultad de Derecho
Centro de Estudios en Libertad de
Expresión y Acceso a la Información





Bertoni, Eduardo Andrés
Internet y derechos humanos II : aportes para la discusión de políticas públicas en América Latina / Eduardo Andrés Bertoni ; compilado por Eduardo Andrés Bertoni. -
1a ed . - Ciudad Autónoma de Buenos Aires : Ediciones del Jinete Insomne, 2016.

200 p. ; 23 x 16 cm.
ISBN 978-987-29629-9-9

1. Internet. 2. Derechos Humanos. 3. Políticas Públicas. I. Bertoni, Eduardo Andrés, comp. II. Título.
CDD 320.6

Universidad de Palermo
Rector
Ing. Ricardo H. Popovsky

Facultad de Derecho
Decano
Roberto Saba

Centro de Estudios en Libertad de Expresión
y Acceso a la Información (CELE)
Director
Eduardo Bertoni

Mario Bravo 1050 (C1175ABT)
Ciudad de Buenos Aires, Argentina
Tel.: (54 11) 5199-4500 (1213)
cele@palermo.edu
www.palermo.edu/cele

Compilador
Eduardo Bertoni

Editado por el CELE, febrero de 2016, Buenos Aires, Argentina

ISBN: 978-987-29629-9-9

Hecho el depósito que marca la ley 11.723.

Impreso en Argentina



Esta compilación de artículos producidos por la Iniciativa por la Libertad de Expresión en Internet del CELE se publica gracias al apoyo financiero de Global Partners Digital.

Índice

Prólogo

iLEI, CELE

En el primer volumen de *Internet y derechos humanos* señalamos que los debates globales sobre regulación de internet se inclinaban hacia la idea de que es necesaria algún tipo de intervención de los Estados en la materia. En esa publicación decíamos, asimismo, que es vital que esto se realice desde una perspectiva de derechos humanos.

En el último tiempo en América Latina han proliferado las iniciativas que buscan regular distintos aspectos de internet. Esta compilación, que reúne los trabajos más recientes de la Iniciativa por la Libertad de Expresión en Internet (iLEI) del CELE, busca ser una herramienta útil en estas discusiones para activistas, legisladores, instituciones académicas y periodistas de la región.

El primero de los artículos, "La gobernanza de internet: la trampa de las formas", propone una mirada crítica sobre el modelo *multistakeholder*, y el rol de los Estados y de la sociedad civil en estos procesos. Lo particular de este trabajo, escrito por Carlos Cortés Castillo, es que entiende a la gobernanza de internet como un espacio de disputa alrededor del control y la gestión de la tecnología más que como un conjunto de instituciones. "La arquitectura de internet es el elemento estructurador más relevante a la hora de analizar cómo estos balances se juegan en la práctica. Lo que queda incorporado en el código de la red difícilmente logra deshacerse a través de negociaciones o diálogos posteriores", dice Cortés Castillo en las conclusiones del artículo y señala que esto debería ser tenido en cuenta por la sociedad civil a la hora de participar en las discusiones sobre cómo se debe gobernar internet.

El artículo que le sigue, "Mercados, propiedad, expresión y uso personal: el sistema de derechos de autor", aborda el tema de los derechos de autor y la necesidad de su replanteo a la luz de los cambios tecnológicos. Modificaciones recientes en legislaciones de propiedad intelectual y debates sobre los

tratados de libre comercio, que van en la dirección de aumentar los plazos de protección en materia de derechos de autor, demuestran que este tema no ha perdido vigencia en la región. “El cambio tecnológico nos motiva a actualizar el derecho positivo para conservar y mantener los valores políticos y sociales que una vez considerábamos importantes, en una especie de modernización del derecho. Pero, a veces, los cambios tecnológicos nos obligan a ir más allá: nos obligan a replantearnos y cuestionar los valores políticos que animan a un sistema jurídico”, señala Meléndez Juarbe.

“El uso de la DMCA para limitar la libertad de expresión”, el artículo siguiente, aborda un tema puntual dentro de los debates sobre propiedad intelectual en la actualidad: el uso indebido de la legislación estadounidense en materia de derechos de autor (la *Digital Millennium Copyright Act, DMCA*) para censurar el discurso crítico en internet en América Latina. El artículo repasa cómo tradicionalmente esta norma ha sido usada de manera indebida para inhabilitar el acceso a contenidos en línea protegidos por los estándares internacionales y regionales de libertad de expresión. La pregunta que se hacen los autores, Eduardo Bertoni y Sophia Sadinsky, es cómo conciliar una norma imperfecta pero necesaria, como la DMCA, con la transgresión de los principios democráticos que esta permite. “Tal vez un tercero independiente, como un grupo asesor internacional, podría contribuir a que se llegue a consensos en esta área tan compleja, aportando pautas neutrales a compañías de internet sobre procedimientos de protección de derechos de autor”, proponen los autores.

Más adelante, esta publicación aborda el tema del mal llamado “derecho al olvido”. Después del fallo conocido como “Google *Spain*” del Tribunal de Justicia de la Unión Europea, surgieron distintas decisiones judiciales e iniciativas legislativas en América Latina que intentan “copiar” esta decisión. A lo largo de este artículo, enfocado en el caso argentino, Verónica Ferrari y Daniela Schnidrig explican por qué trasladar los criterios del fallo europeo a la región puede ir a contramano del sistema interamericano de protección de derechos en materia de libertad de expresión y acceso a la información.

El artículo siguiente, “El ‘internet de las cosas’: más internet que otra cosa” ofrece un panorama general sobre un tema no demasiado abordado hasta el momento por la academia y la sociedad civil en América Latina: los desafíos técnicos que implica hablar de un internet de las cosas (IoT) y los posibles riesgos para los derechos humanos en línea de un entorno de objetos interconectados. “Entre todos los problemas identificados, el de privacidad parece

el más grave. Pensada desde el diseño y la ingeniería, el IoT no incorpora un análisis sobre este punto, a pesar de que la 'privacidad por diseño' no es un tema nuevo en el debate de tecnología y regulación", explica el artículo. Este trabajo de Carlos Cortés Castillo señala, asimismo, que cualquier discusión sobre el tema debe tener en cuenta los retos que todavía persisten en cuanto a infraestructura y acceso a internet en América Latina en tanto la IoT puede profundizar aún más la brecha digital que existe en la región.

Por último, esta publicación presenta un trabajo sobre la regulación de la pornografía no consentida en internet. Este trabajo, elaborado por Paula Vargas de Brea, brinda un panorama de la normativa vigente en Argentina, analiza si se puede aplicar a este tema y, por último, plantea si hace falta otro tipo de regulación que brinde soluciones efectivas y respetuosas de los derechos humanos. El artículo concluye que la pornografía no consentida en internet es de interés regulatorio ya que existe un derecho vulnerado y que debe preverse un mecanismo para su reparación.

Como señalamos antes, esta compilación de artículos busca hacer una contribución a los debates que tienen lugar en la actualidad en la región desde la academia. En línea con los objetivos del CELE, esta publicación se propone ser un insumo para las organizaciones de la sociedad civil, universidades, legisladores y tomadores de decisión involucrados en estas discusiones.

Por último, queremos destacar que esta publicación se realizó gracias al apoyo financiero de Global Partners Digital en el marco de un proyecto en conjunto con el CELE.

Buenos Aires, febrero de 2016

Iniciativa por la Libertad de Expresión en Internet (iLEI),
Centro de Estudios en Libertad de Expresión
y Acceso a la Información (CELE),
Facultad de Derecho, Universidad de Palermo.

La gobernanza de internet: la trampa de las formas

Carlos Cortés Castillo[1]

Resumen

Este documento ofrece una visión crítica sobre la gobernanza de internet pensada para la acción de la sociedad civil. La tesis general es que el debate alrededor de la gobernanza de internet ha estado demasiado centrado en la gobernanza misma antes que en lo que implica.

La primera parte ubica la gobernanza de internet como una configuración de poder y tecnología, y se refiere a los temas principales que la componen. La segunda parte aborda la noción de la participación plural de los actores (el modelo *multistakeholder*) y el rol del Estado. Finalmente, el tercer capítulo hace un comentario de cierre y ofrece una serie de conclusiones y recomendaciones.

I. Introducción

En 1983 internet alcanzó la mayoría de edad. Fue en ese año cuando se implementó el protocolo TCP/IP, según el cual todos los datos en la red se dividen en paquetes y se transmiten por igual a los extremos de esta. Con dicha decisión técnica, la incipiente red militar y académica empezó a expandirse como una telaraña: cientos de redes encontraron caminos entre sí; miles de computadores comenzaron a conectarse.

---

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador de la Iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. Actualmente, es Public Policy Manager en Twitter. La investigación contó con el apoyo de Juan Diego Castañeda.

Arpanet –el antepasado de internet– era hasta entonces un jardín amurallado del que solo hacían parte unos pocos. Para los ingenieros el reto ya no era conectar computadores entre sí, sino lograr que redes distintas interactuaran sin necesidad de intervenirlas o configurarlas. Un cable, un módem, un ordenador y listo. De ahí en adelante la red no pararía de desarrollarse: en 1989 vendría la invención de la *World Wide Web*; en 1993 llegaría el primer navegador apto para gráficas y, dos años después, se privatizarían los puntos principales de conexión, dando lugar a la espina dorsal de la red (el *backbone*).[2]

Hoy, más de 30 años después, la estructura y densidad de internet es mucho más sofisticada. De una población de aficionados y expertos en sistemas pasamos a tener aproximadamente tres mil millones de "ciudadanos" de 194 países.[3] De una red dedicada principalmente al intercambio de correos electrónicos y la navegación de páginas web, pasamos a una de servicios de voz, *streaming* de video y alojamiento de archivos en la nube. De una red compuesta por computadores, pasamos a una interconectada por teléfonos móviles, tabletas, radios y hasta automóviles. De una red compuesta por pocos actores en medio de acuerdos básicos, llegamos a una inmersa en complejas transacciones comerciales. Y, finalmente, de una red desarrollada y manejada por particulares, vamos desembocando en una donde los Estados también quieren ser protagonistas.[4]

Es en este contexto donde se discute el qué y el cómo de la gestión y el control de internet: la gobernanza de internet. No resulta fácil demarcar sus límites, pero tal vez sí sea más sencillo entender lo que está en juego. Alrededor de la pregunta de cómo se gobierna el entorno digital está la respuesta a temas como la protección de la privacidad en línea y el anonimato de los usuarios, el rol de las empresas privadas que controlan la infraestructura de internet, las pretensiones de los Estados nacionales, la responsabilidad de los intermediarios y, claro, la libertad de expresión.

Teniendo en cuenta que existen decenas de libros, manuales y guías sobre gobernanza de internet, escribir algo más sobre el tema puede parecer redundante. Partiendo de ese supuesto, antes que engrosar la lista de estudios

---

2 *Véase*, Hefner, Katie y Lyon, Matthew Lyon, *When Wizards Stay Up Late: The Origins of the Internet,* Nueva York, Simon & Schuste, 1998.

3 *Véase*, Unión Internacional de Telecomunicaciones, "*ITU releases 2014 ICT figures. Mobile-broadband penetration approaching 32 per cent. Three billion internet users by end of this year*", 2014, disponible en: http://bit.ly/1QXoFkq.

4 *Véase*, Yoo, Christopher, *The Diynamic Internet: How Technology, Users, and Businesses are Transforming the Network,* Washington, AEI Press, 2012.

descriptivos, este documento intenta ofrecer una visión crítica pensada, sobre todo, para la acción de la sociedad civil.

La primera parte ubica la gobernanza de internet como una configuración de poder y tecnología, y se refiere a los temas principales que la componen. La segunda parte aborda la noción, transversal a la gobernanza de internet, de la participación plural de los actores (el modelo *multistakeholder*) y el rol del Estado. Finalmente, el tercer capítulo ofrece algunas conclusiones y propuestas.

II. Gobernanza de internet: configuraciones de poder y de tecnología

En 1999 Lawrence Lessig enunció el famoso postulado "el código es ley en internet"[5] para describir la manera en que las reglas informáticas determinan el comportamiento del individuo en el entorno digital. Pero no es el único factor influyente. Para Lessig, al código se suman las leyes, las normas sociales y el mercado. Cohen respondió críticamente a esta teoría: para ella, es errado enunciar estos factores como entes autónomos desplegados o promovidos por actores desinteresados. La configuración del entorno digital, afirma, está inscrita en nuevas formas de ordenamiento social de la emergente sociedad de la información. En ese sentido, las fuerzas que describe Lessig hacen parte de agendas promovidas por distintos actores.[6]

El propio Lessig complementó y contextualizó su teoría en escritos posteriores.[7] Pero más allá de ese debate, acá es posible ubicar un punto de partida para abordar la gobernanza de internet. Las fuerzas económicas y políticas, el mercado y las comunidades de usuarios, ejercen una influencia directa en el diseño y administración de cualquier sistema –incluido internet–. La tecnología "incrusta y está incrustada en prácticas sociales, identidades, normas, convenciones, discursos, instrumentos e instituciones"[8]. Ese campo de disputa es lo que conocemos como la gobernanza de internet.

---

5 *Véase*, Lessig, Lawrence, *Code and Other Laws of Cyberspace,* Nueva York, Basic Books, 1999.

6 *Véase*, Cohen, Julie, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice,* New Haven, Yale University Press, 2012.

7 *Véase*, Lessig, Lawrence, *Code 2.0,* Nueva York, Basic Books, 2006.

8 Jasanoff, Sheila, *"The Idiom of Co -Production",* en: Jasanoff, Sheila (ed.), *States of Knowledge: The Co-Production of Science and Social Order,* Londres, Routledge, 2004, p. 3, citado en: De Nardis, Laura, *The Global War for Internet Governance,* New Haven, Yale University Press, 2014, p. 6. Traducción propia.

Puppis asocia el concepto de "gobernanza" con procesos ciudadanos de participación y deliberación que surgen ante las crecientes dificultades de los Estados para regular los problemas sociales, la fragmentación de poder y de conocimiento, y las nuevas autonomías de distintas partes de la sociedad.[9] En ese mismo sentido, Iosifidis plantea que la diferencia entre gobierno y gobernanza radica en la fuente que ejerce el poder. El Estado es el principal actor en la acción de gobernar, mientras que la gobernanza involucra a varios agentes e implica un poder compartido.[10]

No vale la pena detenerse ahora a buscar una definición exacta de gobernanza –que por demás es esquiva–. Para efectos prácticos, entendemos que se trata de la gestión y el control de una actividad en la que participan múltiples actores –públicos y privados– con intereses contrapuestos. En ese sentido, la gobernanza de internet *"*involucra el diseño y la administración de las tecnologías necesarias para mantener el funcionamiento de internet y la aplicación de políticas sustanciales alrededor de esas tecnologías*"*. En palabras de Mueller, "es la etiqueta más simple, directa e inclusiva para hablar de las actuales disputas y deliberaciones sobre cómo debe coordinarse, administrarse y modelarse internet para reflejar políticas".[11] En la misma línea, Mathiason define la gobernanza de internet como un problema por solucionar. El propósito, afirma, es asegurar que las funciones y los actores que las ejecutan se comporten de tal manera que la red pueda funcionar.[12]

Entender la gobernanza de internet como un juego de equilibrios de poder y un fenómeno social permite alejarse de una visión meramente institucional (sin que ello implique desecharla). Según Van Eeten y Mueller, el área de investigación de este tema ha estado fuertemente atada al estudio de entidades o espacios formales –como ICANN, la Cumbre Mundial sobre la Sociedad de la Información o el Foro de Gobernanza de Internet– donde no necesariamente "sucede" la gobernanza. "Estudiar una institución centralizada es mucho más conveniente que tener que identificar y estudiar la amplia gama de procesos

---

9 *Véase*, Puppis, Manuel, *"Media Governance: A New Concept for the Analysis of Media Policy and Regulation",* en: *Communication, Culture & Critique*, Año 3, Nº. 3, Washington, International Communication Association, 2010, pp. 134-149.

10 *Véase*, Iosifidis, Petros, *Global Media and Communication Policy,* Londres, Palgrave - Macmillan, 2011.

11 Mueller, Milton, *Network and States. The Global Politics of internet Governance,* Massachusetts, MIT Press, 2010, p.9. Traducción propia.

12 Mathiason, John, *Internet Governance. The New Frontier of Global Institutions,* Nueva York, Routledge Global Institutions, 2009.

desarticulados, desordenados y distribuidos globalmente, que producen la gobernanza”[13], explican los autores.

La espina dorsal de la gobernanza de internet es su configuración tecnológica, no solo porque moldea el entorno digital y condiciona la conducta de los usuarios, sino también porque determina el poder de los distintos actores. Se trata de una relación simbiótica: la configuración tecnológica distribuye poder y el poder determina configuraciones tecnológicas.[14] En palabras de Latour, la arquitectura técnica es política por otros medios,[15] exenta de deliberación democrática y proclive a fenómenos de dependencia (*path-dependency*) y consolidación (*lock-in*).

Alrededor de la arquitectura de la red se desarrolla entonces la gobernanza, cuyos debates pasan tanto por la forma como por el fondo: ¿quién toma las decisiones sobre el funcionamiento y la administración de internet?, ¿cómo decide? Antes de estas preguntas hay otras, igualmente complicadas, de carácter metodológico: ¿a qué funciones nos referimos?, ¿existe una lista taxativa?, ¿cuáles son los temas de la gobernanza?

“El propio significado del término ‘gobernanza de internet’ varía a partir de los antecedentes y objetivos de quien lo invoca”[16], afirman Brousseau y Marzouki. “El resultado son muchas ambigüedades y malentendidos a la hora de definir el terreno de juego y los elementos”.[17] A pesar de este nivel de subjetividad, es posible identificar temas recurrentes, aunque no necesariamente excluyentes: (a) recursos críticos de internet; (b) estándares técnicos; (c) acceso e interconexión; (d) seguridad, y (e) regulación de contenidos y propiedad intelectual.[18]

Frente a la gobernanza de cada uno de ellos hay visiones diametralmente opuestas. Mientras algunos actores ven internet como un espacio público

---

13 Van Eeten, Michel, y Mueller, Milton, “*Where is the internet Governance?”*, en: *New Media Society*, Chicago, Universidad de Illinois, 2013, Año: 15, Nº 15, p. 729. Traducción propia.

14 *Véase*, Feenberg, Andrew, *Between Reason and Experience. Essays in Technology and Modernity,* Cambridge, MIT Press, 2010.

15 *Véase*, Latour, Bruno, *The Pasteurization of France,* Cambridge, Harvard University Press, 1998, citado en Musiani, Francesca, “*Network Architecture as Internet Governance”,* en *Internet Policy Review*, Vol. 2, No. 4, disponible en: http://bit.ly/20mvG4b.

16 Brousseau, Eric y Marzouki, Meryem, *“Internet governance: old issues, new framings, uncertain implications”,* en: Brousseau, Eric, Marzouki, Meryem y Cécile Méadel (eds.), *Governance, Regulations and Powers on the Internet,* Nueva York, Cambridge University Press, 2012, p. 368. Traducción propia.

17 *Ibíd.*

18 *Véase*, De Nardis, Laura y Raymond, Mark, *“Thinking Clearly about Multistakeholder Internet Governance”,* ponencia presentada en el Octavo simposio annual GigaNet, Bali, Indonesia, 2013, disponible en: http://bit.ly/1PSiCi9.

donde deben favorecerse el interés general, los derechos humanos y el debate democrático, otros lo entienden como un espacio para innovación e intercambio comercial, sujeto a las leyes del mercado y la libre competencia.[19] Por supuesto, en medio de esas posiciones hay todo tipo de planteamientos.

En el siguiente apartado de este capítulo explicaremos estos temas. Es importante reiterar el objetivo de este documento. Cada uno de estos asuntos es complejo y merece un estudio aparte. Para empezar, en la literatura citada hay un amplio menú para hacerlo. El propósito nuestro, más bien, es ubicar al lector en estos temas para plantear después un debate general sobre la gobernanza de internet.

1. Recursos críticos de internet

Los recursos críticos de internet son una serie de elementos virtuales indispensables para el funcionamiento de la red. Las direcciones de protocolo de internet (*IP addresses*), el sistema de nombres de dominio (*Domain Name System*) y los sistemas autónomos (*Autonomous Systems*), son ejemplos de estos recursos.[20]

Las direcciones IP sirven para identificar cada dispositivo que se conecta a internet con el fin de que el sistema sepa a dónde debe dirigir los datos que el usuario solicita. Debido a su naturaleza, el primer sistema en funcionamiento (IPv4) puede asignar aproximadamente 4,3 billones de direcciones únicas. Hoy ese número se está quedando corto por lo que se busca implementar un sistema (llamado IPv6) que permita una mayor cantidad de direcciones.

Por su parte, el sistema de nombres de dominio surge de la necesidad de usar nombres asequibles para identificar direcciones IP en vez de asociarlas a una extensa retahíla de números. Así, en vez de tener que teclear “72.14.192.0” –un número difícil de recordar– se lo asocia a una dirección en texto. Por ejemplo, www.google.com. El sistema evolucionó de una simple lista en un archivo de texto a una base de datos distribuida en varios servidores.

Los nombres de dominio cuentan con distintas “extensiones” que acompañan la identificación inicial: desde el paradigmático “.com” hasta el “.aero”,

---

19 *Véase*, Brousseau, Eric y Marzouki, Meryem, *supra* nota 16.

20 Para una explicación más detallada de los DNS y el sistema de direcciones IP, ver: Bertoni, Eduardo y Grimani, Atilio, “Nombres de dominio: una expresión que merece ser protegida. Recomendaciones y sugerencias para administradores locales de América Latina y el mundo”, en: Bertoni, Eduardo (comp.), *Internet y derechos humanos. Aportes para la discusión en América Latina,* Buenos Aires, CELE - Universidad de Palermo, 2014.

pasando por ".edu", ".org", ".info", entre otros. Los nombres de dominio están entonces divididos en subgrupos, que en su primer orden se denominan *Generic Top Level Domains* o gTLD. La idea es que todos los nombres de dominio posibles se inserten en uno de esos grupos, cuya administración se entrega a organizaciones privadas que, a su vez, permiten que otras empresas vendan a particulares el registro de dominios concretos. También existen TLD relacionados con países, por ejemplo, ".co" para Colombia o ".ar" para Argentina.

Finalmente, los sistemas autónomos son números binarios que se asignan a cada operador de la red y que, como las direcciones IP, son únicos e indispensables para permitir la conexión entre redes. En otras palabras, es un identificador que se publica o se da a conocer a otros operadores para que sus redes sepan de la existencia de las otras y se interconecten.

Estos recursos se asignan de manera individual y específica a cada persona, dispositivo o red que se conecta a internet. Así, no puede haber dos computadores con la misma dirección IP, dos personas que puedan controlar a la vez un nombre de dominio –como www.wikipedia.org– o dos sistemas autónomos con el mismo identificador. Esta asignación de recursos requiere, por supuesto, de algún tipo de coordinación[21] que hoy en día ejerce la Autoridad de Números Asignados en Internet (IANA, por su nombre en inglés). La IANA es un departamento de –o un conjunto de funciones a cargo de– la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por su nombre en inglés).

A través de IANA, ICANN se encarga de dirigir y autorizar el uso de nombres de dominio y de direcciones IP. Pero no todas las funciones las ejerce directamente. El sistema de nombres de dominio –que, como dijimos, permite encontrar una dirección en un TLD en particular– se encuentra en trece servidores raíz (*root servers*) administrados por empresas o entidades distintas. Por otra parte, cada TLD es manejado también por una empresa u organización diferente a partir de una base de datos llamada "Registro de nombre de dominio", (*Domain Name Registry*). Estos actores privados pueden autorizar a empresas, conocidas como registradores (*registrars*), para que comercialicen los registros entre particulares.

Por último, ICANN delega la asignación de direcciones IP a entidades llamadas *registries* –también conocidas como RIR (*Regional Internet Registry).* Existen cinco y cada una se encarga, en una región del mundo, de asignar

21 *Véase*, De Nardis, Laura, *The Global War for Internet Governance,* New Haven, Yale University Press, 2014.

números en bloque a prestadores de servicio de internet para que puedan ofrecerlos a sus clientes.

Existen varios problemas frente a los recursos críticos. Mencionaremos acá tres de ellos. El primero se refiere al mercado de los gTLD. A diferencia de las direcciones IP o los sistemas autónomos, y de acuerdo con lo explicado anteriormente, los gTLD se pueden comprar y vender como cualquier producto comercial. Esto implica que entre más gTLD haya, más comercialización y productos habrá. Esto pone en jaque a las empresas dedicadas a defender los derechos de propiedad intelectual. Para estos actores resulta inconveniente que haya demasiados gTLD, ya que implica tener más frentes abiertos –todos los dominios relacionados con su marca, por ejemplo– para defender.[22] Pero no solo los particulares tienen intereses económicos en la materia sino que también para ICANN representa un beneficio, pues cobra 185 000 dólares por estudiar la posibilidad de crear y entregar al solicitante un nuevo gTLD.[23]

Por otro lado está la cuestión de la pluralidad en el lenguaje de los TLD. Los caracteres con los que se escriben se ajustan al estándar estadounidense para el intercambio de información (ASCII, en inglés). Por esta razón, caracteres en otros idiomas –como la letra "ñ"– no hacen parte de los TLD. Esto ha generado una tensión entre países y grupos culturales para quienes internet debe reflejar la pluralidad de lenguas distintas al estándar ASCII. ICANN ha estudiado el problema balanceando ventajas y desventajas de incluir otros caracteres dentro de los TLD.[24] Por ahora, autorizó el registro de 31 gTLD en caracteres en árabe, chino y ruso.[25]

Finalmente, identificamos el problema de las direcciones IP relacionado con el asunto de los contenidos. En ocasiones, titulares de *copyright* en Estados Unidos logran rastrear dónde terminan descargadas sus obras gracias a las direcciones IP. Basados en este dato, buscan que los jueces autoricen la entrega de los datos personales del usuario al que corresponde ese identificador. Por ahora las autoridades de ese país no han aceptado dicha pretensión y consideran que la dirección IP no equivale a la identidad de un supuesto infractor.[26] Los titulares de *copyright* buscan que este recurso crítico pueda

---

22 *Véase*, Mueller, Milton, *Ruling the Root*, Cambridge, MIT Press, 2002.

23 *Véase*, ICANN, *Applicant Guidebook,* Versión 2012-06-04, p.1-42, disponible en: https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf.

24 *Véase*, ICANN, *"Discussion Paper on Non-ASCII Top-Level Domain Policy Issues",* disponible en: http://bit.ly/1o2t6PJ, última consulta: 15 de agosto de 2014.

25 *Véase*, ICANN, *"Delegated strings",* disponible en: http://bit.ly/1c9EADr, última consulta: 15 de agosto de 2014.

26 *Véase*, Van der Sar, Ernesto, "*Judge: IP-Address is Not a Person and Can't Identify a Bittorrent*

usarse como una herramienta de control frente al uso no autorizado de sus contenidos.

2. Establecimiento de estándares técnicos

Así como las vías públicas requieren reglas para que cada automóvil pueda llegar seguro del punto A al punto B, en internet se emplean reglas –llamadas protocolos– para recibir y transmitir información y, en general, para que el sistema funcione. La principal preocupación que subyace a la creación de protocolos es la interoperabilidad, es decir, la posibilidad de que todos los operadores y aplicaciones del sistema funcionen bajo las mismas reglas.

El protocolo más importante para internet se denomina TCP/IP (*Transmission Control Protocol/Internet Protocol*), y es el que indica para dónde van los datos, cómo se dividen en paquetes y cómo deben rearmarse en su lugar de destino. Además de éste, existen otros como SMTP, para transmisión de correos electrónicos, FTP para transmisión de archivos y HTTP, para la transmisión de páginas web.[27]

El diseño de protocolos de internet está a cargo del Grupo de Trabajo de Ingeniería de Internet (IETF, por su nombre en inglés), una organización informal de personas con interés y conocimiento técnico suficiente para proponerle a sus pares estas reglas técnicas. Por su parte, el World Wide Web Consortium (W3C) es el organismo encargado de determinar estándares para el funcionamiento de la web.

Un debate relevante frente a la definición de estándares tiene que ver con la forma como éstos afectan el derecho a la privacidad en el entorno digital. Por ejemplo, el TCP/IP –el protocolo básico de la red– impone el trato igualitario de paquetes y datos, y desarrolla el principio de "extremo a extremo", lo cual, en principio, resulta más amigable para la privacidad de los usuarios. De manera similar, pero en un nivel distinto de jerarquía en la red, el protocolo para el intercambio de archivos BitTorrent está diseñado para evitar la conservación de registros de direcciones IP, haciendo más difícil la persecución de quienes lo usan. Las características de estos protocolos, y en especial aquellos

Pirate", disponible en: http://bit.ly/1matN83, última consulta: 18 de agosto de 2014.

27 Para una explicación básica de los protocolos de internet y, en particular, del TCP/IP, vea: Cortés, Carlos, "La neutralidad de la red: la tensión entre la no discriminación y la gestión" y "Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en internet", en: Bertoni, Eduardo (comp.) *Internet y derechos humanos. Aportes para la discusión en América Latina,* Buenos Aires, CELE – Universidad de Palermo, 2014.

que configuran la arquitectura original de internet, son objeto de críticas y presiones. Por distintas razones –seguridad, *copyright*, prevención del crimen– desde muchas orillas se propone reformarlos para que resulte más fácil identificar a los usuarios.

Por otro lado, recientemente el W3C anunció que incluiría dentro del estándar web la protección de contenidos por medio de DRM (*Digital Rights Management*), una serie de códigos informáticos que evitan la copia, modificación o usos no autorizados de cualquier contenido protegido por *copyright*. Los DRM, en general, someten los contenidos a un control casi perfecto por parte de sus propietarios, mucho más allá de lo que permiten las leyes sobre derecho de autor.[28] Por esa razón, el anuncio de W3C levantó muchas críticas, que, en síntesis, apuntan a un desmedro del dominio público y los usuarios en favor de una industria en particular.[29]

3. Acceso e interconexión

Internet es una red de redes. Esto quiere decir que su carácter global –esa economía de escala que la define– depende de que los operadores de cada red lleguen a acuerdos para interconectarse. Para el efecto, los prestadores del servicio de red tienen tres opciones generales: (i) vender la interconexión a operadores de menor tamaño y conectarse, en principio de forma gratuita, a otras redes de su mismo nivel; (ii) comprar a las redes de primer nivel la interconexión y venderla a los de tercer nivel; o, (iii) sólo comprar la interconexión al segundo nivel para proveerla a sus clientes.

No obstante, los incentivos para mover datos y los distintos tipos de aplicaciones han propiciado la aparición de nuevos intermediarios y servicios. Hoy existen, por ejemplo, los puntos de intercambio de tráfico (*Internet Exchange Points,* o IXP), las redes de distribución de contenidos (*Content Delivery Networks*) y las "granjas de servidores", que al igual que las redes más tradicionales, buscan acuerdos con los prestadores del servicio de internet para llevar el contenido al usuario final.[30]

Más allá de los problemas y retos técnicos, la complejidad de la red importa en términos de gestión y administración. Los acuerdos entre todos estos

---

28 *Véase,* Cohen, Julie, *"Pervasively Distributed Copyright Enforcement",* en: *The Georgetown Law Journal*, Vol. 95:1, Washington, Georgetown University, 2006, p 2 y ss.

29 O'Brian, Danny, *"Lowering Your Standards: DRM and the Future of the W3C",* disponible en: http://bit.ly/KxLL1I, último acceso: 18 de agosto de 2014.

30 *Véase*, Yoo, Christophe, *supra* nota 4.

actores son privados; se han llevado a cabo por fuera de contextos normativos tradicionales y están motivados y estructurados por intereses económicos particulares antes que mandatos técnicos o provisiones de interés público. El primer interés de ellos es ofrecer servicios exclusivos –mejor remunerados y de calidad más alta– para usuarios con expectativas comerciales muy claras. Y aunque muchas de esas prácticas puedan satisfacer a un público determinado, ponen en riesgo la unidad y carácter común de la red.[31]

La solución de estos problemas es sumamente compleja. Algunos expertos sugieren la creación de un régimen público de interconexiones –como las autopistas y vías de un país– o la imposición de tarifas estándar de intercambio de tráfico para evitar prácticas anticompetitivas. Estas propuestas, sin embargo, no han logrado dar cuenta de la cantidad de actores emergentes, la escala y diversidad de los acuerdos privados existentes, y el tipo de solución aplicable. A fin de cuentas, un temor fundado en toda la regulación de la tecnología y la innovación, es que se imponga una solución que, como una camisa de fuerza, atente contra la misma evolución de la red.[32]

4. Seguridad

De la seguridad de la red dependen los operadores y los usuarios. Los ataques de denegación de servicio (conocidos como *Denial of Service Attacks, DoS* o *DDoS*), el robo de información, la suplantación de identidad, el uso de *spyware*, y una larga lista de riesgos, son una realidad en el entorno digital. De la mano con la expansión de la red y la llegada de nuevos servicios, vienen también los problemas en materia de seguridad.

La seguridad de internet toca una lista innumerable de asuntos: tiene que ver con consideraciones sobre integridad de datos, autenticación y confidencialidad de usuarios, prevención de accesos no autorizados, detección y respuesta ante ataques informáticos, confianza de los usuarios para hacer pagos en línea y la amplia agenda de la seguridad nacional de los Estados.[33]

---

31 *Véase*, Chapin, Lyman, "*Interconnection and Peering among Internet Service Providers",* en: *Interisle White Paper*, 2005, disponible en: http://bit.ly/1JVtklF.

32 *Véase*, Faratin, Peyman y otros, "*The Growing Complexity of Internet Interconnection"* en: *Communications & Strategies*, No. 72, Cambridge, Akamai, 2008;. *Véase también,* Yoo, Christopher, *supra* nota 4.

33 *Véase*, Doria, Avri, *"What do the Words 'Internet Security' Mean?", en*: Kleinwächter, Wolfgang, *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment,* Berlín, Springer, 2007.

El sector comercial –del que también hacen parte las empresas que ofrecen las soluciones a estos riesgos– suelen ser reiterativas al hablar de la cantidad de dinero que se pierde por cuenta de la inseguridad en línea.[34] Y aunque el problema existe y no debe ser subestimado, el discurso de la seguridad, al igual que el del *copyright,* es sobre todo favorable a los intereses de ciertos jugadores. Las arquitecturas de control –como planteábamos antes– tienen detrás una agenda de distribución de poder y determinación de conductas.[35]

La seguridad en la red ha sido tema de discusión en las instituciones formales de la gobernanza de internet[36]. Las soluciones varían tanto en términos técnicos como políticos. Están, por ejemplo, los grupos nacionales de respuesta rápida (CERT, por su nombre en inglés), los certificados de autenticidad de servicios y aplicaciones, y las propuestas para mejorar la seguridad en el núcleo del diseño de la red (protocolos de seguridad como DNSSec o IPSec).

Desde el punto de vista de la gobernanza de internet, el problema básico –como muchos en esta área– es la dificultad para coordinar a los grupos de interés. Los Estados tradicionalmente han sido responsables de mantener la seguridad de sus ciudadanos pero hoy se encuentran actuando como iguales dentro de un grupo de actores no estatales, acordando reglas y métodos más allá de su mandato legal y sus posibilidades prácticas. [37]

La posibilidad de centralizar el control en el Estado tampoco parece viable. La configuración abierta y descentralizada de internet y su incorporación social dispersa y múltiple imponen un camino igualmente distribuido en materia de seguridad. Que los gobiernos impulsen regulaciones concentradas y centralizadas alrededor de su poder punitivo no solo resulta poco práctico e ineficiente, sino que, al igual que en otros casos, puede propiciar cambios estructurales negativos en el entorno digital, en detrimento de la libertad de expresión, la privacidad y otros derechos fundamentales.[38]

---

[34] *Véase,* Brenner, Joel, "*Eyes wide shut: The growing threat of cyber attacks on industrial control systems",* en: *Bulletin of the Atomic Scientists,* No. 69 (5), Sage Journals, 2013.

[35] *Véase,*Cohen, Julie, *supra* nota 6. .

[36] *Véase,* Gupta, Arvin y Samuel, Cherian, "*A Comprehensive Approach to Internet Governance and Cybersecurity",* en: *Strategic Analysis*, Vol. 38, No. 4, Nueva Delhi, IDSA, 2014.

[37] Mueller, Milton, Schmidt, Andreas, y Kuerbis, Brenden, "*Internet Security and Networked Governance in International Relations",* en: *International Studies Review,* 2013.

[38] *Véase,* Deibert, Ronald, *Black Code: Inside the Battle for Cyberspace,* Toronto, McClelland & Stewart, 2013.

5. Regulación de contenidos y propiedad intelectual

No existe un tema sobre el cual haya mayor expectativa que la regulación de los contenidos en línea. Tanto los Estados como los actores privados enfrentan en internet el riesgo de la pérdida de control frente a qué contenidos intercambian los usuarios, para qué los usan y cómo lo hacen. Los motivos varían de la misma forma que las estrategias. Por razones políticas, comerciales o simplemente estratégicas (que no son tema de este documento), unos y otros recurren a la tecnología –apoyada por la regulación o los acuerdos entre particulares– para ponerle cerrojos a la red.

Existen muchas tecnologías que permiten bloquear o filtrar contenidos: la inspección profunda de paquetes, que permite discriminar el destinatario, el emisor o el contenido de la transmisión; el bloqueo de dominios, que impide la consulta de un sitio web en particular; la inhabilitación de sitios o servicios por medio de ataques de denegación del servicio, o la instalación de filtros en puntos de acceso de la red, como el prestador del servicio o el "ama de llaves" de un grupo de computadores.[39]

El control técnico puede tener como fuente una ley, un tratado internacional –como veremos en el siguiente tema– o un acuerdo privado. Estas medidas, además, suelen combinarse con imposiciones operativas a los intermediarios, como son las licencias de funcionamiento o los registros obligatorios (para, por ejemplo, tener un cibercafé).[40] Cuando el Estado no tiene poder directo sobre los medios técnicos que facilitan la conexión, como sucede en la mayoría de los casos, debe presionar los puntos donde pueda realizar un control efectivo. Esos puntos son los intermediarios de internet que prestan servicios de conexión (como Claro o Telmex), de información (Google o Yahoo!), de acceso a contenidos (YouTube), o de transacciones financieras (PayPal y bancos tradicionales).[41]

---

39 Para una explicación completa de los diferentes medios técnicos para bloquear o filtrar contenidos, véase Murdoch, Steven y Anderson, Ross, "*Tools and Technology of Internet Filtering*", en:Deibert, Ronald y otros, *Access Denied,* Cambridge, MIT Press. 2008.

40 *Véase,* Zittrain, Jonathan y Palfrey, John, "*Internet Filtering: The Politics and Mechanisms of Control",* en: *ibíd.*

41 *Véase,* Wu, Tim y Goldsmith, Jack, *Who controls the Internet?. Illusions of a Borderless World,* Oxford, Oxford University Press. 2008. *Véase también*, Cortés, Carlos, "Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital", en: Bertoni, Eduardo (comp.), *Internet y derechos humanos. Aportes para la discusión en América Latina,* Buenos Aires, CELE - Universidad de Palermo, 2014.

También se pueden imponer usos de la tecnología –que en última instancia consiguen el objetivo final de control del contenido– desde su fase de diseño. Es el caso de los DRM, mencionados anteriormente, que imponen, por ejemplo, que un archivo de música o video solo pueda usarse en un dispositivo aprobado o por un tiempo determinado. Lo mismo sucede con el software que restringe ciertos usos en un computador o los programas que supervisan la actividad del usuario con el propósito de que se ajuste a la actividad autorizada.[42]

Todas estas medidas encuentran en la industria del *copyright* un ferviente promotor. Desde la Organización Mundial del Comercio (OMC) se vienen discutiendo tratados internacionales para que el uso de obras en el entorno digital quede reducido, como decíamos antes, únicamente a las modalidades que autorice el propietario. Recientemente se ha propuesto crear una regulación transnacional vía acuerdos comerciales dentro de los que se destacan el Acuerdo Comercial Anti-Falsificación (ACTA, por su nombre en inglés) y el Acuerdo Estratégico TransPacífico de Asociación Económica (TPP, también por su nombre en inglés).

De manera complementaria, diversos Estados han adoptado leyes para ofrecerle al titular del material un procedimiento expedito para retirar contenidos de internet. La regulación pionera en la materia y modelo de muchas otras es el DMCA (*Digital Millenium Copyright Act*) de los Estados Unidos. Estos regímenes han suscitado críticas entre los usuarios de internet y académicos, para quienes esas soluciones resultan desproporcionadas y contrarias al debido proceso y la libertad de expresión.[43]

Además de lo relacionado con las creaciones protegidas por *copyright*, también existe un pulso por intervenir la gestión de recursos en favor de los derechos de propiedad intelectual (lo cual también se relaciona con el primer literal de este capítulo). La principal fuente de tensión es la asignación de nombres de dominio, los cuales se registran en favor de quien primero los solicite. Este parece ser un método eficiente en vista del volumen de peticiones que se formulan a diario.[44] Sin embargo, ha suscitado el descontento de los

---

42 *Véase*, Zittrain, Jonathan, *The Future of Internet and How to Stop It,* New Haven, Yale University Press – Penguin UK, 2008.

43 *Véase*, entre otros, Lessig, Lawrence, *Free Culture,* Nueva York, Penguin Books, 2004; Vaidhyanathan, Siva, *Copyrights and Copywrongs: The Rise of Intellectual Property and How it Threatens Creativity,* Nueva York, NYU Press, 2003; Patry, William, *Moral Panics and the Copyright Wars,* Oxford, Oxford University Press, 2009.

44 *Véase*, Mueller, Milton, *supra* nota 11.

titulares de marcas que llegan tarde para registrar un dominio determinado. Por ejemplo, un particular registra www.mcdonalds.com en vez de la cadena de hamburguesas. Para resolver este problema, ICANN y la OMC diseñaron un sistema de resolución de disputas por nombres de dominio (UDRP, por su nombre en inglés) que busca defender al titular de una marca registrada y entregarle el nombre de dominio relacionado que otro haya registrado.[45]

El debate sobre el control de contenidos atraviesa todos los temas de la gobernanza de internet. Es un medio y un fin en sí mismo, y se juega en múltiples escenarios y con diversos jugadores. Desde un punto de vista más general, su importancia reside en la fuente del control y la manera como lo instrumentaliza. Las tensiones suelen plantearse desde la perspectiva de los gobiernos y las leyes que impulsan con el propósito de controlar la información en línea. Sin embargo, los particulares, como subrogados del Estado o por cuenta propia, cumplen un papel igualmente relevante. Allí, los medios se vuelven invisibles: el código define la regulación del contenido y la regulación de este contenido está en un contrato al que el usuario se adhiere con un clic.

III. El rol del Estado, los particulares y el modelo *multi-stakeholder*

La mayoría de teorías acerca de la globalización suelen compartir el lugar común de la decadencia del Estado. Según estas, la globalización socava la soberanía nacional y debilita la habilidad de los gobiernos para regular sus asuntos domésticos. Por otro lado, la globalización empodera a los actores no estatales debido a la reducción de costos de transacción entre fronteras y la posibilidad de trabajo en red.[46]

Estos presupuestos parecen diseñados a la medida de internet, un fenómeno globalizado por naturaleza. Los Estados se ven limitados por su competencia territorial mientras que internet no conoce fronteras; alrededor de internet surgen nuevas formas de acción, colaboración y participación, mientras que los Estados tienen una capacidad limitada para intervenir. Las comunicaciones son masivas y cambiantes y la respuesta del Estado difícilmente se acopla a la velocidad y evolución de la tecnología.[47]

---

45 *Véase*, ICANN, "Acerca de las disputas sobre nombres de dominio", disponible en: http://bit.ly/1Q9HpbR, última consulta: 19 de agosto de 2014.

46 *Véase*, Drezner, Daniel, *All Politics Is Global. Explaining International Regulatory Regimes,* Nueva Jersey, Princeton University Press, 2007.

47 *Véase*, Mueller, Milton, *supra* nota 11.

Para Drezner, si en algún escenario deberían evidenciarse a plenitud los efectos de esa globalización arrolladora tendría que ser internet. Por supuesto, ese no es el caso. Del ciberentusiasmo del siglo pasado solo queda el recuerdo. Las palabras de Nicolás Negroponte –*"Internet no puede ser regulado. No es que las leyes no sean relevantes; es que el Estado-Nación no es relevante."*–[48] o la declaración de independencia del ciberespacio que hiciera John Perry Barlow en 1996, son cosa del pasado.[49] Hoy en día la globalización de internet pasa por muchos factores de poder y la intervención del Estado se da por descontada.

Sería fácil concluir que las intervenciones de los gobiernos en internet se dividen entre aquellos que son democráticos y aquellos que no. En un extremo están Alemania, Estados Unidos o Inglaterra, cuya intervención solo busca garantizar los derechos fundamentales y propiciar un entorno de confianza para las relaciones comerciales. En el otro aparecen países como China, Cuba o Irán, cuyo propósito de controlar la red no es otro que coartar las libertades individuales, vigilar a los ciudadanos y favorecer los intereses del partido en el poder.

El asunto, claro, es más complejo. Aunque es posible identificar gobiernos que abiertamente consideran internet una amenaza para su estabilidad y proyecto político, entre el amplio grupo de países democráticos hay visiones contradictorias sobre el tipo de intervención estatal que amerita. Los contenidos ofensivos en línea, por ejemplo, han merecido respuestas regulatorias en países como Alemania o Francia, pero no en Estados Unidos. Los sitios de apuestas en línea, en cambio, no merecen ninguna respuesta en Europa, pero son sistemáticamente bloqueados en Estados Unidos.[50]

La regulación de los gobiernos funciona imponiendo costos y cargas y, en los casos más graves, también como un sello hermético. Lo cierto es que para intervenir en internet los Estados no han tenido que salir de sus fronteras; ha sido suficiente, como explicábamos anteriormente, con imponerles obligaciones a los intermediarios de internet –las "amas de llaves"– que se asientan en

---

48 The Guardian, *"China Begins to Erect Second Great Wall in Cyberspace"*, 5 de febrero de 1996, citado en: Drezner, Daniel, *supra* nota 46, p. 94.

49 "Gobiernos del Mundo Industrial, ustedes, gigantes cansados de carne y acero, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, les pido a ustedes, del pasado, que nos dejen en paz. No son bienvenidos entre nosotros. No tienen soberanía donde nos reunimos". Barlow, John Perry, *"A Declaration of Independence of Cyberspace",* disponible en: http://bit.ly/1KUdsea, última consulta:11 de agosto de 2014. Traducción propia.

50 *Véase*, Murray, Andrew, *The Regulation of Cyberspace. Control in the Online Environment,* Nueva York, Routledge-Cavendish, 2007.

su territorio. De esta forma, con distintos niveles de éxito y dependiendo del país, se han hecho presentes en el entorno digital.[51]

Esto no quiere decir que ahora la red esté supeditada a la autoridad exclusiva de los Estados, o que los actores privados hayan perdido relevancia.[52] La realidad histórica, como explica De Nardis, es que "la mayoría de funciones de la gobernanza de internet no han sido de domino de los gobiernos, sino que han sido ejecutadas a través de órdenes privadas, diseño técnico y nuevas formas institucionales".[53]

De este pulso entre gobiernos y particulares surge el modelo *multi-stakeholder* –o de pluralidad de participantes interesados– de la gobernanza de internet. La Agenda de Túnez para la Sociedad de la Información lo describe en estos términos:

> Una definición de trabajo de la gobernanza de internet es desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de internet.[54]

De la Chapelle considera que la gobernanza *multi-stakeholder* es necesaria para abordar asuntos transfronterizos como internet, ya que permite apalancar estructuras diversas como los gobiernos, las organizaciones de la sociedad civil, las empresas y las organizaciones internacionales. Dicho de otra forma, vuelve interoperables los distintos marcos de gobierno existentes. *"*La gobernanza *multi-stakeholder* puede promover la democracia, enriquecer estructuras representativas existentes y empoderar a los ciudadanos en nuestro mundo interconectado e interdependiente*"*.[55]

El modelo *multi-stakeholder* (usamos el término en inglés a falta de una palabra precisa en español) se ha convertido en el referente del tema, el eje transversal a todas las áreas. Cuando se habla de gobernanza de internet en espacios internacionales, es usual que enseguida se enuncie el modelo

---

51 *Véase,* Goldsmith, Jack y Wu, Tim, *supra* nota 41.

52 *Ibíd.*

53 *Véase*, De Nardis, Laura, *supra* nota 21.

54 WSIS, *Agenda de Túnez para la sociedad de la información,* WSIS-05/TUNIS/DOC/6(Rev.1)-S, 2006, disponible en: http://bit.ly/1PSjt2i, última consulta: 11 de agosto de 2014.

55 De La Chapelle, Bertrand, "*Multistakeholder Governance: Principles and Challenges of an Innovative Political Paradigm"*, en: *MIND, Multistakeholder Internet Dialogue*, Berlin, Co:-llaboratory, 2011, No. 1, p. 9. Traducción propia. *Véase*, De Nardis, Laura, *supra* nota 21, p. 265.

multi-stakehoder como el camino a seguir. Una participación plural, horizontal y abierta –se dice– es la única forma de gobernar internet.

De Nardis y Raymond critican que este modelo se presente como algo innovador e inherente a las particularidades de internet, lo cual lo vuelve un fin antes que un medio. Así, el objetivo deja de ser la preservación de la interoperabilidad, estabilidad, seguridad y apertura de la red, para convertirse en la aplicación de la herramienta. Por otra parte, los autores consideran que el modelo *multi-stakeholder* puede no ser el adecuado para cada área funcional de la gobernanza de internet. Es decir, no es la 'talla única' para los problemas de administración y gestión de la red.[56]

El modelo *multi-stakeholder* en este ámbito hace mucho énfasis en que existan lugares o instancias donde todos los actores estén convocados para hablar y proponer. Y entre más participación haya, mejor. Se parte de alguna forma del supuesto de que si el escenario está diseñado para hablar de gobernanza de internet, habrá gobernanza de internet. Pero, como suele evidenciarse en estos espacios, ni son todos los que están, ni están todos los que son.

Para Van Eeten y Mueller, esta perspectiva idealista:

> (…) ignora decisiones estratégicas que los actores hacen sobre en qué escenarios participarán y cuáles ignorarán, evitarán o boicotearán. Estos cálculos, basados en un interés propio básico, se vuelven extremadamente importantes cuando los actores tienen el control verdadero de un recurso y hay verdaderas pérdidas o ganancias como resultado de decisiones colectivas obligatorias.[57]

Las definiciones sobre la gestión y el control de internet se dan necesariamente en espacios donde las partes tienen algún incentivo para sentarse a interactuar y buscar acuerdos. Y en los escenarios *multi-stakeholder* los convocados que tienen algún nivel de poder no llegan con la idea de jugárselo en una mesa de trabajo.[58]

El Foro de Gobernanza de Internet (IGF, por su nombre en inglés) es el escenario más conocido para el diálogo entre diversas partes interesadas. Sin embargo, desde su concepción la idea fue –recuerdan Van Eeten y Mueller– tener un lugar de intercambio donde no se pudieran tomar decisiones, impulsar mandatos o publicar conclusiones.[59] Para algunos, en esto consiste su

---

56 *Véase*, De Nardis, Laura y Raymond, Mark, *supra* nota 18.

57 *Véase,* Van Eeten, Michel y Mueller, Milton, *supra* nota 13, p. 728. Traducción propia.

58 *Véase,* Van Eeten, Michel y Mueller, Milton, *supra* nota 13.

59 *Véase*, *Ibíd*.

atractivo: “como nada saldrá de ahí, todos los asistentes pueden poner de lado por unos días sus pretensiones, alianzas, políticas formales e intereses, y simplemente hablar”.[60] El problema, evidente para muchos asistentes habituales a los IGF es que las discusiones cándidas y espontáneas –salvo por algunos integrantes de la sociedad civil– terminan siendo elaboradas estrategias de relaciones públicas.

En abril de 2014 tuvo lugar en Brasil Net Mundial, la “Reunión global de múltiples partes interesadas sobre el futuro de la gobernanza de internet”.[61] Con el evidente interés del gobierno de Dilma Rousseff de introducir a su país entre los pesos pesados de este tema, la reunión convocó a 1 480 personas entre representantes de gobiernos, organismos multilaterales, empresas y sociedad civil. A diferencia del IGF, la conclusión de Net Mundial fue un documento *multi-stakeholder* que abarca todas las áreas relacionados con internet. En particular, manifiesta que “las decisiones sobre gobernanza de internet en ocasiones se toman sin la participación significativa de todos los actores relevantes. Es importante que la toma de decisiones y formulación de políticas *multi-stakeholder* mejore para asegurar una participación completa de todas las partes interesadas”.[62]

El documento fue objetado por 27 organizaciones de la sociedad civil, para quienes el resultado de la conferencia no refleja preocupaciones clave como la neutralidad de la red, la vigilancia masiva o la protección de la libertad de expresión.[63] En otras palabras, ese grupo manifiesta lo que el mismo documento había identificado como un problema: la falta de participación de ellos como actores de relevantes. Al parecer, varios gobiernos, entre ellos el de Estados Unidos, dieron un pulso para que varios de estos puntos estuvieran débilmente presentes en la versión final.[64]

La representación de la sociedad civil en el modelo *multi-stakeholder* adolece además de una contradicción interna, y es la diferencia de visión entre las

---

60 McGarry, Dan, “*Talking Shop”,* disponible en: http://bit.ly/1Pdp5Pc, última consulta: 18 de agosto de 2014.

61 *Véase*, http://bit.ly/1QXueiZ, última consulta: 18 de agosto de 2014.

62 Net Mundial, “*Net Mundial Multistakeholder Statement*”, 2014, disponible en: http://bit.ly/1nLhMBC. Traducción propia.

63 *Véase,* Best Bits, *“Civil society closing statement at NETmundial 2014*”, disponible en: http://bit.ly/1SqjNGm, última consulta: 18 de agosto de 2014. Otras organizaciones, como la Asociación para el Progreso de las Comunicaciones, destacaron avances que se lograron en la reunión. Véase, “*Association for Progressive Communications (APC) statement on NETmundial*”, disponible en: http://bit.ly/1iQsV4c, última consulta: 19 de agosto de 2014.

64 *Véase,* Dourado, Eli, “*NETmundial wrap-up*”, disponible en: http://bit.ly/1UGnQf4, última consulta: 18 de agosto de 2014.

organizaciones más cercanas a los movimientos de derechos humanos y aquellas vinculadas a la comunidad técnica. La aproximación de esta última suele seguir el esquema inicial de desarrollo de la red, aún presente en algunas de las instituciones que definen estándares y recursos: autorregulación, consenso y permanencia de los principios y valores base de internet. Por su parte, las organizaciones con un enfoque más político y legal, plantean discusiones amplias en términos del ejercicio de derechos fundamentales y controles democráticos. A pesar de que existen objetivos comunes en varios de estos grupos, las expectativas y metas divergen en muchos puntos.[65]

Un último problema del modelo *multi-stakeholder* se relaciona con la causa a la que puede terminar sirviendo. En muchos escenarios, las demandas de participación amplia hacen parte de una crítica al poder de Estados Unidos en la administración de ciertas funciones de la red –como se vio anteriormente–. En este sentido, para De Nardis "las aproximaciones *multi-stakeholder* que buscan la promoción de la democracia pueden convertirse en una carrera por el más bajo común denominador sobre qué es un valor democrático aceptable".[66] Al final del día, un modelo con una pluralidad mayor de participantes podría abrirle campo a países como Rusia o China para que –siguiendo sus valores democráticos y usando su músculo político– promuevan una visión de internet ajena a la que de manera preponderante tiene la sociedad civil, al menos en América Latina.

IV. Conclusión y recomendaciones

Este capítulo abordó la gobernanza de internet desde la relación entre configuraciones tecnológicas y configuraciones de poder. Ese acercamiento crítico busca tomar distancia del enfoque tradicional de las metodologías y las formas. La gobernanza de internet, antes que el conjunto de instituciones y fórmulas multilaterales de discusión, es un campo de disputa alrededor del control y la gestión de una tecnología.

El estudio de la gobernanza de internet debe abrirse entonces a todos aquellos que ejercen poder en la red, sin importar el escenario en el que se encuentren. Hacer este esfuerzo requiere identificarlos, entender el tipo de interés que tienen y la forma como influyen en el entorno digital –si administran un recurso crítico o si hacen parte de la infraestructura, por ejemplo–.[67]

---

[65] *Véase*, Brousseau, Eric y Marzouki, Meryem, *supra* nota 16.
[66] *Véase*, De Nardis, Laura, *supra* nota 21, p. 230.
[67] *Véase,* Van Eeten, Michel y Mueller, Milton, *supra* nota 13.

Esa visión –sociológica, si se quiere– puede dar luces sobre las motivaciones y expectativas de quienes participan en la gobernanza de internet, y sobre los puntos de presión y los elementos en disputa. Sin embargo, enfrenta la limitación de no poder responder a la pregunta de cómo debe ser la gobernanza de internet. Mucho menos puede responder esta pregunta el acercamiento común a este tema, en el cual la gobernanza de internet es, sobre todo, la descripción de una serie de procesos.

Esto parece indicar que la gobernanza de internet no es del todo útil para saber cómo gobernar internet. Como lo demuestran las fuentes consultadas para este documento sí resulta útil para describir arreglos institucionales, herramientas de decisión y grupos de interés alrededor de internet. Pero como marco de referencia para abordar problemas y para proponer soluciones desde la sociedad civil, parece insuficiente.

Para avanzar en una aproximación nueva de la gobernanza de internet –incluso evitando esta etiqueta como disciplina– es necesario desintegrar el concepto de internet para, más bien, abordar las tensiones que existen en el entorno digital en diferentes frentes. Una aproximación realista de internet, plantea Mozorov, debe evitar la reivindicación de valores inherentes –como la transparencia, la apertura– para prestarle particular atención a cómo esos valores se manifiestan en debates específicos.[68]

Buscar un trabajo más táctico no equivale a desconocer que existe una visión hacia donde debe propender una tecnología como internet. Para De Nardis y Raymond, "un acercamiento apropiado para una gobernanza de internet responsable y eficaz requiere determinar qué tipos de administración son óptimas para promover un balance de interoperabilidad, innovación, libertad de expresión y estabilidad operativa en cualquier contexto funcional y político".[69]

La arquitectura de internet es el elemento estructurador más relevante a la hora de analizar cómo estos balances se juegan en la práctica. Lo que queda incorporado en el código de la red difícilmente logra deshacerse a través de negociaciones o diálogos posteriores.[70] Así, el seguimiento a las fuerzas que moldean esa infraestructura y la manera como toman las decisiones, debe ser una prioridad para la sociedad civil.

---

[68] *Véase*. Morozov, Evgeny, *To Save Everything, Click Here: The Folly of Technological Solutionism,* Nueva York, PublicAffairs, 2013.

[69] *Véase*, De Nardis, Laura y Raymond, Mark, *supra* nota 18, p. 2. Traducción propia.

[70] V*éase*, Musiani, Francesca, "*Network Architecture as Internet Governance",* en *Internet Policy Review*, Vol. 2, No. 4, disponible en: http://bit.ly/205Y98Y.

Hasta hoy la sociedad civil –abusando de la generalización– ha promovido la fórmula del diálogo *multi-stakeholder* como la avenida para enfrentar esos retos. Sin embargo, como se expuso acá, los actores relevantes no llegan a esos escenarios –si es que realmente asisten– con la intención de reevaluar su posición de poder en la red o de aceptar un cambio que consideren adverso a sus intereses. Antes que seguir reprochando esa actitud hay que entenderla y enfrentarla. Entender esa limitación del modelo *multi-stakeholder* implica, en otros palabras, "dejar de verlo como un fin en sí mismo que deba ser aplicado de manera homogénea a todas las funciones de la gobernanza de internet".[71]

Ilustremos este punto con el ejemplo del *copyright.* Desde distintos frentes los agentes interesados en extender la protección del derecho de autor al entorno digital –incluso más allá de lo que originalmente pretendía proteger– vienen promoviendo cambios en todas las capas de la red. Los instrumentos para hacerlo se combinan y retroalimentan: tratados internacionales, leyes, gestión de derechos (*Digital Rights Management*) y asignación de recursos críticos. Sin embargo, las fuerzas no están del todo alineadas a su favor: la sociedad civil también promueve protocolos, pero para hacer más fácil el intercambio de contenidos; los Estados tramitan leyes de responsabilidad de intermediarios que no necesariamente siguen la agenda de las industrias creativas, y otras empresas igualmente poderosas se inclinan por entornos digitales menos coercitivos.

En ese contexto, la apuesta por un diálogo *multistakeholder* sin matices no solo es una pérdida de tiempo, sino también una vía que en última instancia puede favorecer a quienes esperan tomar todas las decisiones a puerta cerrada. En un escenario tan complejo como el del *copyright* la sociedad civil debe elevarles a los actores interesados los costos de tomar decisiones a espaldas del interés público, debe buscar los caminos propicios para cuestionar las negociaciones, debe indagar por las modificaciones en el código, y debe litigar los cambios y movilizar a la gente para que los exija. Por supuesto, nada de lo que se acaba de decir es novedoso: muchos grupos ya están inmersos en una tarea similar. El problema, sin embargo, es que montados en la bicicleta estática de los escenarios formales de la gobernanza y el diálogo multisectorial, muchos esfuerzos de coordinación e incidencia se pierden.

Por último, subyace la pregunta sobre el papel del Estado. De un lado, las organizaciones de la sociedad civil les exigen un rol pasivo en el entorno digital. Del otro, esperan una intervención activa en la preservación de los derechos fundamentales y en la supervisión de los intermediarios más poderosos.

---

[71] *Véase*, De Nardis, Laura y Raymond, Mark, *supra* nota 18, p. 2. Traducción propia.

Aceptar una visión heterogénea de la gobernanza de internet también pasa por asimilar y abrazar esa paradoja: necesitamos exigirle distintos roles al Estado en el entorno digital. Y, de la misma forma, necesitamos que los Estados entiendan que su papel en la gestión y control de internet varía según el contexto. Mantener un entorno seguro para las transacciones en línea no implica acabar con la privacidad, o asegurarse de que los intermediarios respeten los derechos fundamentales en los servicios que prestan no requiere estatizar la red.

Al final será imposible controlar todos los factores que influyen en el gobierno de internet. La descentralización de actores y la dispersión del control, en últimas, permiten, por ahora, que nadie tenga todo el poder para llevar este tren en una u otra dirección. Tal vez el rol de la sociedad sea hacer ese ejercicio de equilibrismo.

Mercados, propiedad, expresión y uso personal: el sistema de derechos de autor

Hiram Meléndez Juarbe[1]

Resumen

Los cambios tecnológicos nos obligan a replantearnos y cuestionar los valores políticos que animan a un sistema jurídico. Actualizar el derecho positivo en materia de derechos de autor nos obliga a reflexionar en torno a cómo lo imaginamos, para qué lo queremos, qué intereses sociales e individuales debe reflejar y si su fundamentación debe reconsiderarse.

El presente capítulo propone cuatro paradigmas de derecho de autor, visiones de mundo sobre lo que es y debe ser este régimen de derecho: mercado, propiedad, expresión y uso personal. Estos paradigmas están en permanente tensión, sobre todo en algunos espacios –legales y tecnológicos– como pueden ser la responsabilidad de los intermediarios o los DRM. Proponemos aquí una discusión sobre qué intereses se busca priorizar a la hora de actualizar el sistema de derechos de autor.

---

1 Este artículo fue escrito por Hiram A. Meléndez Juarbe, catedrático asociado de la Escuela de Derecho de la Universidad de Puerto Rico. J.D., U.P.R. (2000); LL.M., Harvard Law School (2002); LL.M., New York University (2008); J.S.D., N.Y.U. (2013). Este escrito fue preparado para la conferencia "Hacia una reconceptualización de los derechos de autor II" organizada por el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo, Buenos Aires, celebrada el 21 de octubre de 2014.

I.

Hoy día se impone la pregunta: ¿qué valores debe reflejar un sistema de derechos de autor?[2] En general, replantearse en voz alta los objetivos de la norma jurídica es, como mínimo, una forma de mantenerla en el espacio de deliberación pública para cuestionarnos si responde a nuestras necesidades, aspiraciones y realidades. Pero hay razones especiales por las que esta pregunta es crucial en el contexto de los derechos de autor.

Todas y todos hemos escuchado que los cambios tecnológicos contemporáneos ponen presión a ciertas normas jurídicas y la fundamentación detrás de ellas. Sonará trillado, pero no deja de ser cierto; particularmente en aquellas áreas del derecho que inciden sobre la producción y transmisión de información –como es el caso del derecho a la privacidad y la libertad de expresión– frecuentemente encontramos que tanto la norma jurídica, así como sus objetivos, tienen que ser replanteados ante realidades materiales y tecnológicas cambiantes.

En este sentido, el cambio tecnológico nos motiva a actualizar el derecho positivo para conservar y mantener los valores políticos y sociales que una vez considerábamos importantes, en una especie de modernización del derecho.[3] Pero, a veces, los cambios tecnológicos nos obligan a ir más allá: nos obligan a replantearnos y cuestionar los valores políticos que animan a un sistema jurídico.

Pensemos, por ejemplo, en el derecho a la privacidad. En una concepción muy tradicional, ese derecho sirve para protegernos contra intromisiones en nuestro entorno más secreto y privado: aquello que cuidamos celosamente y que protegemos ante la vista de otros (a diferencia de información que divulgamos al público). Hoy día, sin embargo, muchos exigimos alguna protección a información sobre nosotros mismos, aun cuando la hayamos publicado y divulgado masivamente (en redes sociales, por ejemplo). El reclamo de un derecho a la privacidad en público es, en cierta forma, un llamado a reconocer valores políticos repensados y rearticulados a la luz de cambios tecnológicos.

---

2 Cuando menciono la existencia de un sistema de derechos de autor, lo hago haciendo referencia a uno de mis escritos previos. *Véase,* Meléndez Juarbe, Hiram, "Tecnopolítica y derechos de autor", en: Do Amaral Júnior, Alberto, *El Constitucionalismo en transición,* Buenos Aires, Libraria, 2011.

3 Lawrence Lessig sugirió que en ocasiones nos limitamos sólo a esa modernización porque se delega la responsabilidad de forjar estructuras jurídicas a personas con poca imaginación: nosotros, los abogados. *Véase,* Lessig, Lawrence, *Code and Other Laws of Cyberspace,* Nueva York, Basic Books, 1999.

De esta forma, hoy día podemos asociar el derecho a la privacidad no sólo con lo privado y secreto, como es tradicional, sino más ampliamente con la libertad de expresión y con el interés de controlar cómo nos proyectamos en público y nos relacionamos con otros.[4] Así, vemos cómo los cambios tecnológicos requieren que repensemos la norma y, además, sus valores fundantes.

Lo mismo pasa con un sistema de derechos de autor. Preguntarse cómo actualizarlo ante estos cambios debe incluir, pues, una reflexión en torno a cómo lo imaginamos ampliamente, para qué lo queremos, qué intereses sociales e individuales debe reflejar y si su fundamentación debe reconsiderarse.

II.

Tradicionalmente pensamos en dos posibles justificaciones para un sistema de derechos de autor. Por un lado, la protección al autor se concibe como una forma de crear incentivos; un estímulo para la generación de obras por vía de derechos exclusivos de propiedad para la autora o el autor –propiedad cuyo modo de distribución preferido es el mercado, según esta visión–. Por otro lado, la protección al autor se concibe como un derecho personal, de índole moral. El autor o autora se merece una protección, ya sea porque existe una conexión entre la obra y él o ella, o porque merece que se reconozca el expendio del sudor de su frente.

Por eso pensamos en los fundamentos de un sistema de derechos de autor activando un binomio de intereses (patrimoniales y morales) que tienen como eje central al autor o autora. Quiero proponer, sin embargo, que el panorama es y debe ser más complejo. Y quiero proponer, además, que las tecnologías de información contemporáneas nos invitan a incorporar intereses que coloquen en el centro del sistema, no sólo al autor, sino también –de forma prominente– al usuario de las obras y a la comunidad en general.

Nótese que he estado hablando de un sistema de derechos de autor. Es un sistema, en buena medida, porque es pluralista: refleja y debe reflejar, conjugar y negociar las presiones que imponen varios grupos de valores que aspiran a dar fundamentación a este régimen de derecho. De modo que un sistema

---

[4] *Véase,* Meléndez Juarbe, Hiram, “La Constitución en ceros y unos: un acercamiento digital al derecho a la intimidad y la seguridad pública”, en: *Revista Jurídica de la Universidad de Puerto Rico*, No. 77, San Juan, UPR, 2008, p. 45 y ss. *Véase también,* Meléndez Juarbe, Hiram, “El derecho a la intimidad, nuevas tecnologías y la jurisprudencia del juez Hernández Denton: Lo público de lo público”, en: *Revista Jurídica de la Universidad de Puerto Rico*, No. 83, San Juan, UPR, 2014, p. 1035 y ss.

de derechos de autor es un conjunto de valores en conflicto constante, por lo que no debemos afirmar que tiene que promover un único objetivo.[5] No se trata, pues, de proteger uno o algunos de estos intereses y valores, sino de buscar formas para conjugarlos todos armónicamente.

A estos conjuntos de valores los llamo paradigmas de derecho de autor –visiones de mundo sobre lo que es y debe ser este régimen de derecho–. Yo identifico cuatro paradigmas importantes: mercado, propiedad, expresión y uso personal.

Dependiendo de la jurisdicción, algunos de éstos se reflejarán claramente en el derecho positivo, en la fundamentación de las decisiones judiciales y en la estructura del derecho de autor. Otros se recogen más tenuemente, a mayor o menor grado, y se defienden o rechazan vigorosamente en el debate público, en los tribunales, y en espacios académicos. El punto no es que todo sistema jurídico en efecto recoja de igual forma esta combinación de valores o paradigmas, o que los refleje a todos de algún modo. Es obvio que no. El punto, en cambio, es que los operadores jurídicos (jueces, legisladores, forjadores de política pública, activistas, académicos) explícitamente traten a su régimen jurídico como un sistema que combine diversas visiones de mundo (yo propongo estas cuatro) y hagan transparente cuál es la configuración que su sistema propone, qué sacrificios se hacen, cuáles valores quedan descartados y por qué.

III.[6]

Conforme a la visión de mundo que llamo el *Paradigma del mercado*, el derecho de autor aspira a maximizar el bienestar social brindando incentivos

---

5 *Véase,* Meléndez Juarbe, Hiram, *supra* nota 2. Para otras visiones pluralistas *véase,* Merges, Robert, *Justifying Intellectual Property,* Cambridge, Harvard University Press, 2011. *Véase también,* Fisher III, William , "*Theories of Intellectual Property"*, en: Munzer, Stephen R. (ed.), *New Essays in Legal and Political Theory of Property,* Cambridge, Cambridge University Press, 2001. *Véase también,* Tehranian, John, *Infringement Nation. Copyright 2.0 and You,* Oxford, Oxford University Press, 2011, pp. 54-57. *Véase también,* Fromer, Jeanne C., "*Expressive Incentives in Intellectual Property*", en: *Virginia Law Review*, No. 98, Charlotesville, Virginia Law Review Association, 2012, pp. 1745-1746. *Véase también,* McGowan, David, "*Copyright Nonconsequentialism"*, en: *Missouri Law Review*, Vol. 69, No. 1, Columbia, University of Missouri School of Law, 2004. *Véase también,* Burk, Dan L., "*Law and Economics of Intellectual Property: In Search of First Principles*", en: *Annual Review of Law and Social Science,* Vol. 8, Palo Alto, Annual Reviews, 2012, pp. 397-414.

6 Esta discusión se basa en mi ensayo, "Tecnopolítica y derechos de autor", *supra* nota 2. Abandono aquí el concepto de *Paradigma de incentivo* usado en ese escrito para hablar del *Paradigma del mercado* por ser más apropiado y descriptivo. Incluyo, además, el *Paradigma de uso personal* como uno independiente.

suficientes a productores de información, evitando el *free riding* que se produciría en la ausencia de los derechos exclusivos (en atención al carácter intangible de las obras intelectuales). Pero como la innovación es acumulativa, la creación intelectual de una persona es un producto de su proceso creativo, así como un factor de producción para otros creadores subsiguientes. Por eso, la obra intelectual tiene un valor social que excede el valor privado para el primer creador.

Bajo esta visión, el alcance y duración del derecho de autor dependerá de cuánto creemos que estas externalidades de la innovación beneficiarán a creadores posteriores en sus propios procesos creativos. Por tanto, el mayor reto con la privatización de recursos intelectuales está en asegurar la producción de este bien público mientras se limita el derecho para evitar que sea subutilizado.

De acuerdo a esta versión, el individuo es imaginado como escogiendo entre posibilidades que maximicen su utilidad. Por supuesto, los autores crean por razones distintas a la recompensa económica directa y persiguen intereses creativos por diversas razones como, por ejemplo, su deseo de comunicarse, respeto de pares y reconocimiento.[7] Generalmente, este paradigma opera *ex ante*: es decir, como un incentivo antes de la creación, y se usa para justificar aquellas protecciones al autor en la medida que sea necesario para inducir la producción. Esta postura *ex ante*, por lo tanto, puede justificar un tipo de protección minimalista, pues justificaría sólo aquellas protecciones que sean necesarias para inducir al autor, y no más que eso. Pero el Paradigma del Mercado podría –y frecuentemente lo hace– dar base a justificaciones maximalistas *ex post*[8] bajo la idea de que el control casi absoluto de todas las facetas de una

---

7 *Véase,* Leenheer Zimmerman, Diane, "*Copyrights as Incentives: Did We Just Imagine That?"*, en: *Theoretical Inquiries in Law,* Tel Aviv, Tel Aviv University, No. 12, 2009, p. 29 y ss. El *Paradigma del mercado*, y su idea complementaria del individuo, no da cuenta apropiadamente de la producción por pares (*peer-to-peer*) o los muchos casos de innovación no remunerada por usuarios. *Véase también*, Von Hippel, Eric, *Democratizing Innovation,* Cambridge, MIT Press, 2005. Otros, sin cuestionar esta imagen de lo que motiva la innovación, cuestionan sin embargo si el monopolio de la propiedad aumenta el bienestar, o *welfare. Véase también,* Boldrin, Michelle y Levine, David K., *Against Intellectual Monopoly,* Cambridge, Cambridge University Press, 2008.

8 *Véase,* Lemley, Mark, "*Ex Ante versus Ex Post Justifications for Intellectual Property",* en: *The University of Chicago Law Review,* No.71, Chicago, Chicago University, 2004, p.129 y ss. Se argumenta que sólo derechos de propiedad intelectual fuertes brindan a un creador incentivos adecuados para innovar y mejorar sobre obras existentes a través del tiempo debido a que ellos están posicionados para recibir las señales del mercado sobre versiones iniciales de las obras. Se alega, además, que la protección fuerte previene que se desgaste el valor de los derechos de propiedad intelectual. *Véase también,* Picker, Randal C., "*Fair Use v. Fair Access"*,

obra en el futuro propende al bienestar social –como cuestión de eficiencia asignativa– y, por lo tanto, resulta más eficiente concentrar en unas manos la decisión sobre el destino de esa obra[9] –en comparación con otras alternativas más distribuidas–. Esta visión *ex post* se traduce en excepciones limitadas a favor de los usuarios, una protección vigorosa a las obras derivadas[10] o la extensión prolongada del término de protección, entre otras cosas.

Le llamo el *Paradigma del mercado* pues el proceso creativo tiene al mercado como alfa y omega: la promesa del mercado da vida a la obra, es su consecuencia natural y su modo de distribución ideal. El mentado incentivo es, precisamente, para que la obra pueda traficarse como un bien de consumo. El objetivo último –el bienestar social– es posible aquí tras la satisfacción de preferencias de los individuos que quisieran la obra pagando su precio, la cual ha de producirse porque existe la posibilidad de su consumo. Se trata, pues, de la comodificación absoluta del derecho de autor y del proceso creativo.[11]

Cuando hablo del *Paradigma moral de propiedad*, por otro lado, me refiero a una dimensión moral. Es muy fácil trasladarse de una concepción de mercado a una visión de merecimiento moral.[12] Como expresó Jeremy Waldron, "[e]l pensamiento se mueve de estímulo, a incentivo, a beneficio, a recompensa, a merecimiento, de manera que algo que comienza como un asunto de política social deseable acaba siendo concebido como un derecho moral"[13].

Este *Paradigma moral de propiedad* toma varias formas. Por un lado, como mencioné, se justifica la propiedad intelectual como moralmente merecida, a

---

en: *The Columbia Journal of Law and the Arts,* No. 31, Nueva York, Columbia Law School, 2007, p. 603 y ss. Landes, William y Posner, Richard, *The Economic Structure of Intellectual Property Law,* Cambridge, Harvard University Press, 2003.

9 *Véase,* U.S., Eldred c/ Ashcroft, 537 U.S. 186 del 15 de enero de 2003, disponible en: http://bit.ly/1JVvtO4. *Véase también,* Epstein, Richard A., "*The Disintegration of Intellectual Property? A Classical Liberal Response to a Premature Obituary"*, en: *Stanfort Law Review,* No. 62, Stanford, Stanford Law School, 2009, p. 455 y ss. *Véase también,* Epstein, Richard A., "*What is So Special about Intangible Property? The Case for Intelligent Carryovers*", en: Manne, Geoffrey A. y Wright, Joshua D. (eds.), *Competition Policy and Patent Law under Uncertainty*, Cambridge, Cambridge University Press, 2010, p.42 y ss.

10 *Véase,* Abramowicz, Michael, "*A Theory of Copyright's Derivative Right and Related Doctrines"*, en: *Minnesotta Legal Review, Vol.* 90, Minneapolis, 2005, p. 317 y ss.

11 *Véase,* Radin, Margaret Jane , *Contested Commodities,* Cambridge, Harvard University Press, 1996.

12 Para una discusión reciente sobre justificaciones no consecuencialistas a la propiedad intelectual *véase,* Merges, Robert, *supra* nota 5.

13 Waldron, Jeremy, "*From Authors to Copiers: Individual Rights and Social Values in Intellectual Property",* en: *Chicago-Kent Law Review,* Vol. 68, Chicago, IIT Chicago-Kent College of Law, 1993, pp. 841-851.

partir de la mezcla del trabajo individual con recursos comunes[14] o a partir de una conexión entre la obra y la personalidad del autor[15]. Esta visión encuentra eco, por ejemplo, en la protección de derechos morales de autor, tales como los derechos de atribución e integridad. Este último impide que terceros –aun cuando adquieran legalmente copias de la obra– realicen alteraciones que puedan afectar la reputación y dignidad del autor. Pero el *Paradigma moral de propiedad* va más allá de este tipo de norma en el derecho positivo. Tiene un arraigo profundo en la cultura y se manifiesta en la idea de que, sobre todas las cosas, el autor o autora moralmente merece algún tipo de derecho de propiedad.

Es pertinente aquí precisar tres asuntos fundamentales al *Paradigma moral de propiedad*. Primero, en el contexto de los derechos de autor, así como en otros, la propiedad puede entenderse discursivamente. Como propone Carol Rose, la propiedad es persuasión: es decir, un ejercicio discursivo en el que continuamente imaginamos, discutimos e intentamos convencer a otros en torno a las maneras de concebir el uso, disfrute y distribución de las cosas.[16] Imaginar a la propiedad de esta manera, discursivamente, como un constructo social, nos permite explorar su maleabilidad y revelar las luchas que se dan para constituir, cambiar o reconfigurar su significado.

El segundo punto es que ese ejercicio discursivo tiene un impacto tangible y profundo sobre nuestras vidas. Ello porque, a partir de estos procesos, quedan constituidas categorías jurídicas. Estas, a su vez, contribuyen a forjar nuestras identidades.[17] Es decir, nuestra identidad –nuestro contenido de consciencia, cómo nos visualizamos, cómo vemos al mundo, quiénes somos frente a otros– queda influenciada, entre otras cosas, por el contenido que se

---

14 *Véase,* Gordon, Wendy, "*A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property",* en: *Yale Law Journal,* Vol. 102, New Haven, 1993, p. 1533 y ss. *Véase, además*, Attas, Daniel, "*Lockean Justifications of Intellectual Properties*", en: *Gosseries, Axel, Marciano, Alain y Strowel, Alain (eds.), Intellectual Property and Theories of Justice*, Nueva York, Palgrave Mcmillan, 2008.

15 *Véase,* Hughes, Justin, "*The Philosophy of Intellectual Property"*, en: *Georgetown Law Journal,* Vol. 77, Washington D.C., Georgetown University Law Center, 1988, p. 287 y ss. Sobre los derechos morales en general *véase*, Rigamonti, Cyrill P., "*Deconstructing Moral Rights"*, en: *Harvard International Law Journal,* Vol. 47, 2006. En los Estados Unidos *véase,* Visual Artists Rights Act of 1990, 17 USC §§ 101, 106A, disponible en: http://bit.ly/1NODsax. *Véase también,* Rosenthal Kwall, Roberta, "*Inspiration and Innovation: The Intrinsic Dimension of the Artistic Soul"*, en: *Notre Dame Law Review,* Vol. 81, Notre Dame, Notre Dame Law School, 2006.

16 *Véase,* Rose, Carol M., "*Canons of Property Talk, or, Blackstone's Anxiety"*, en: Yale Law Journal, Vol. 108 New Haven, 1998, pp. 601- 622.

17 *Véase,* Rivera Ramos, Efrén, "Derecho y subjetividad", en:, *Fundamentos,* No. 5-6, 1997-98, p. 125 y ss.

le dé discursivamente a la propiedad privada, y por la forma en la que queda incorporado ese contenido formalmente en el derecho.[18]

De ahí que, por el carácter que discursiva y legalmente toma la propiedad y, por ende, el carácter que toma el *Paradigma moral de propiedad*, se constituye la identidad del autor de la obra, concibiéndoselo como una persona esencialmente virtuosa. Como contraparte, se construye la identidad del usuario no autorizado a quien se lo percibe fundamentalmente como un pirata. De modo que el uso no autorizado y el individuo que lo realice adquiere un carácter de inmoralidad.[19]

Todo esto queda evidenciado por las agresivas campañas "educativas" para representar todas las copias no autorizadas como ilegales y, por lo tanto, todos los que realizan esa práctica como ladrones y piratas.[20]

El tercer punto es que ese usuario no autorizado que queda constituido y retratado por el *Paradigma moral de propiedad* –el pirata o ladrón– produce, a su vez, una suerte de usuario que es imaginado como virtuoso: me refiero al usuario como consumidor. Y es aquí que el *Paradigma moral de propiedad* refuerza al *Paradigma del mercado*. Si bien el usuario no autorizado de la obra es conceptualizado como un pirata inmoral, el usuario virtuoso es el que paga por ella.

Comprender esta construcción de sujetos virtuosos y no virtuosos es crucial porque, en un sistema de derechos de autor saludable, el *Paradigma moral de propiedad* –y los sujetos virtuosos y no virtuosos que produce: el autor, el pirata y el consumidor– puede y debe tener competencia.

Otros paradigmas, el de *Expresión* y el de *Uso personal*, entre otras cosas, proveen alternativas que incorporan valores sociales particularmente importantes en un entorno digital.

---

18 *Véase, Ibíd. Véase también,* Bourdieu, Pierre, "*The Force of Law: Toward a Sociology of the Juridical Field"*, en: *Hastings Law Journal,* Vol. 38, San Francisco, UC Hastings College of the Law, 1987, p. 805 y ss. *Véase también,* Fontánez Torres, Érika, *Ambigüedad y derecho: Ensayos de crítica jurídica,* Cabo Rojo, Editora Educación Emergente, 2014.

19 *Véase*, Peñalver, Eduardo Moisés y Katyal, Sonia K., *Property Outlaws: How squatters, pirates, and protesters improve the law of ownership,* New Haven, Yale University Press, 2010. *Véase también,* Cohen, Julie, "*The Place of the User in Copyright Law"*, en: Fordham Law Review, Vol. 74, Nueva York, Fordham University School of Law, 2005, p. 347-351.*Véase también,* Waldron, Jeremy, *supra* nota 13, p. 842. Como expresa Waldron, "[s]i pensamos en un autor como alguien que posee un derecho natural a enriquecerse de su obra, entonces pensaremos en quien copia como una especie de ladrón". Traducción propia.

20 *Véase,* Palfrey, John, y Gasser, Urs, *Born Digital: Understanding the First Generation of Digital Natives,* Nueva York, Basic Books, 2008, p. 137. Para más información, *véase*, la página web de la Copyright Alliance Education Foundation, http://bit.ly/1o2yOkw. *Véase también,* Anderson, Nate, "*EFF gives copyright education a crack with new curriculum",* disponible en: http://bit.ly/1UGoIjP.

El *Paradigma de expresión* imagina a otro tipo de usuario. Sabemos que un régimen de libertad de expresión debe contribuir a sostener condiciones para un discurso público vigoroso.[21] Pero en la medida que los paradigmas de *Mercado* y de *Propiedad* refuerzan una visión mercantilizada del derecho y del proceso creativo colocando en el centro del universo al autor, existe un riesgo real de que se afecte adversamente el discurso público si el sistema de protección impide que los usuarios se expresen a través de obras que circulan en su entorno cultural y que ostentan un poder simbólico significativo. El *Paradigma de expresión*, y el tipo de sujeto expresivo que concibe, debe servir de contrapeso a estas presiones.

Este paradigma a veces es visto como parte del esquema de incentivos, particularmente la visión minimalista *ex ante* porque, conforme a esta, solamente se justifican aquellas protecciones necesarias para incentivar la creación y se favorecen limitaciones que permitan a otros crear sobre ellas, en una especie de espiral creativo.[22] En consonancia con esta visión, casi todos los sistemas tienden a permitir una variedad de usos no autorizados toda vez que estos usos puedan verse conectados a valores de libertad de expresión. Así, por ejemplo, doctrinas como la de *fair use*, la de *fair dealing* y otras excepciones permiten el uso de obras sin permiso para un sinfín de objetivos expresivos, tales como educativos[23], investigación, políticos, críticas y parodias, entre otros.[24]

En cierto sentido, el *Paradigma de expresión*, así articulado, tiende a enfatizar la importancia de la producción de información por el usuario y su contribución a un mercado de ideas y a la calidad del debate público. Por ello, tienden a valorarse aquellos usos que sean transformativos o "constructivos", o que pueda decirse que contribuyen al entorno expresivo más amplio –a diferencia de, por ejemplo, la apropiación que no tenga como resultado una contribución pública o la transformación en algo nuevo–.[25] Así, el usuario

---

[21] *Véase,* Post, Robert, *Constitutional Domains: Democracy, Community and Management,* Cambridge, Harvard University Press, 1995.

[22] *Véase,* Harper y Row c/ Nation Enterprises, 471 US 539, 558, del 20 de mayo de 1985 ("*the Framers intended copyright itself to be the engine of free expression. By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas.*"). *Véase también*, McGowan, David , *supra* nota 5.

[23] Para la relación entre el entorno educativo y los valores de libertad de expresión, *véase*, Post, Robert, *Democracy, Expertise, Academic Freedom: A First Amendment Jurisprudence for the Modern State,* New Haven, Yale University Press, 2012.

[24] 17 USC. § 107, *supra* nota 15.

[25] *Véase,* Eldred c/ Ashcroft, *supra* nota 9, pp 186-221, (resaltando el menor valor constitucional de "*mak[ing] other people's speeches*"). *Véase también*, Netanel, Neil, *Copyright's Paradox,* Oxford, Oxford University Press, 2008.

privilegiado en este modelo es imaginado, en palabras de Tushnet, dentro del "discurso constitucionalizado más tradicional sobre crítica contestataria, protesta, ofensa y la expresión impopular"[26]. El sujeto virtuoso aquí es aquel que tiene algo que decir y contribuir al discurso público, pero lo dice tomando prestadas palabras de otros.[27]

El *Paradigma de uso personal*, por el contrario, tiene como eje al individuo y su interacción con el contenido. En este sentido, contrario al *Paradigma de expresión*, el de *Uso personal* valora la experimentación personal y privada sin tener en cuenta si contribuye o no algo nuevo al entorno expresivo.[28] Me refiero a prácticas con una dimensión menos exteriorizada tales como abrir, editar, recombinar, manipular obras, simplemente explorarlas y jugar con ellas, así como actividades relacionadas e incidentales –como romper candados digitales que impidan estos usos personales–.

Estas prácticas de uso personal pueden concebirse sobre la base de alguna teoría de autonomía individual y como parte de procesos de autodefinición personal.[29] Pero podrían también anclarse en una visión que subraya el carácter situado (no tanto autónomo) de los sujetos, como hacen Julie Cohen y Madhavi Sunder.[30] Es decir, el tipo de usuario imaginado por el *Paradigma de uso personal* es un sujeto que está sumamente inmerso en, atado a, y arropado por su contexto cultural. Esta persona juega con los elementos culturales que le constituyen, en procesos iterados y en un toma y dame continuo con la cultura. Pero el sujeto aquí está situado en un sentido que no es estático, pues no se le concibe como vinculada permanentemente al contexto cultural tal cual existe –como los sería tal vez bajo una concepción de la cultura vista como tradición–.[31] En vez, el sujeto opera a través de la cultura, nadando a través de

---

26 Tushnet, Rebecca, *"Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It"*, Yale Law Journal, Vol. 114, 2004, pp. 535-587.

27 *Ibíd.*, p. 560.

28 *Véase,* Tushnet, *supra* nota 26.

29 Estos valores de autonomía se destacan hoy en el contexto de tecnologías digitales, pues las condiciones materiales para la producción y manipulación de productos culturales permiten identificarnos y experimentar personalmente con ellos como participantes activos de procesos culturales y no como receptores pasivos de información. *Véase*, Balkin, Jack, "*Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society"*, NYU Law Review, Vol. 79 , Issue 1, Nueva York, New York University School of Law, 2004. *Véase también,* Tushnet, Rebecca, *supra* nota 26, p. 565.

30 *Véase,* Cohen, Julie, *Configuring the Networked Self,* New Haven, Yale University Press, 2012. *Véase también,* Sunder, Madhavi, *From Goods to a Good Life: Intellectual Property as Global Justice,* New Haven, Yale University Press, 2012.

31 Sunder, Madhavi, *Ibíd.*

ella –dice Cohen, "*working through culture*"[32]– de modo que su ubicación le permite experimentar con ella, con la posibilidad de trascenderla, transgredirla y reconfigurarla. En fin, el usuario situado consume obras digitales, las copia para uso personal o, conforme al *Paradigma de expresión*, para comunicar a otros. Las apropia para experimentar, jugar, reinventarse personalmente y, si quiere, proponer. La cultura es, en este paradigma, un proceso generativo que oscila entre la estabilidad de los elementos culturales que tenemos –estabilidad necesaria para anclarse en un contexto para experimentar– y la transgresión de lo que puede ser. La cultura es también participativa, pues depende de sujetos situados que trabajen a través de ella, desde su vientre.

En la medida que el *Paradigma de uso personal* también sirve como precondición, en ocasiones necesaria, para la expresión pública, podemos ver su íntima conexión con el de *Expresión*. Así, en el contexto de la Constitución de los Estados Unidos, por ejemplo, la Primera Enmienda debe exigir que ambos paradigmas se vean reflejados en su sistema de derechos de autor.[33]

Un sistema de derechos de autor debe, como mínimo, reflejar estos paradigmas y proveer mecanismos para que se regulen mutuamente. Sus interrelaciones pueden ser sumamente complejas. Por ejemplo, si bien el *Paradigma del mercado* presume de la comodificación de las obras y del proceso creativo, y si bien el *Paradigma moral de propiedad* lo refuerza con la construcción del pirata, la realidad es que el binomio *Mercado/Propiedad* refleja una situación híbrida, en lo que Margaret Jane Radin llama "comodificación incompleta",[34] pues en muchas partes los derechos morales se conciben como inalienables y, por lo tanto, como limitantes al mercado.[35]

Y desde el punto de vista del usuario y sus intereses como agente expresivo o como sujeto situado, los paradigmas de *Expresión* y de *Uso personal*

---

32 Cohen, Julie, *supra* nota 30.

33 Esta es la tesis central de un trabajo en progreso, Meléndez Juarbe, Hiram, *Copyright, Personal Use and the First Amendment: A Public Discourse Perspective,* a 2013.

34 Jane Radin, Margaret, *supra* nota 11.

35 Como ejemplo están las leyes de Francia, España y México. Véase, Code de la propriété intellectuelle [C. Pr. Int.] Art. L. 121-1, Francia: "*Il est perpétuel, inaliénable et imprescriptible.*", énfasis suplido. *Véase también,* Texto Refundido de la Ley de Propiedad Intelectual Art. 14 (B.O.E. 1996, 1/1996), España: "Corresponden al autor los siguientes derechos irrenunciables e inalienables". *Véase también,* Ley Federal del Derecho de Autor [LFDA - Federal Copyright Act], según enmendada, Art. 19, Diario Oficial de la Federación, 24 de diciembre de 1992, México: "El derecho moral se considera unido al autor y es inalienable, imprescriptible, irrenunciable e inembargable". *Véase también*, Creative Commons Puerto Rico, *Moral Rights in Puerto Rico and the Puerto Rico V.3.0 Creative Commons License*, San Juan, 2007, disponible en: http://bit.ly/1QELTKa.

deben servir de contrapeso a las presiones que ejercen los de *Mercado* y *Propiedad*. De modo que, por ejemplo, si bien debemos favorecer arreglos legales que estén orientados a incentivar la creación con derechos de propiedad, por su impacto contra el uso expresivo por terceros, también debemos hacer un esfuerzo consciente por limitar la protección a aquellos incentivos que sean absolutamente necesarios para su creación –la versión *ex ante*, y no la versión *ex post*– y la protección de amplias libertades de uso bajo mecanismos como el *fair use* y otras limitaciones y excepciones. Si bien el discurso público vigoroso en un régimen de libertad de expresión se promueve con la producción y divulgación de obras creativas protegidas por derechos de autor, también se sostiene con la protección de la expresión de usuarios que echan mano de su entorno cultural inmediato.

Ahora bien, si aceptamos como válidas y aceptables las retóricas de *Mercado* y de *Propiedad* en un sistema pluralista, aunque estas deben estar limitadas por los paradigmas de *Expresión* y de *Uso personal*, estos últimos dos también son condicionados y estructurados por los primeros. Por eso, como dije antes, los paradigmas de *Expresión* y de *Uso personal* deben existir como contrapeso y no para cancelar absolutamente los de *Mercado* y de *Propiedad*. No todo uso sin permiso debe ser privilegiado: realmente existen piratas y villanos, aunque no todos lo seamos. Pero entiendo que sí deben ser privilegiados los usos personales que cataloguemos como no comerciales así como los usos expresivos, transformativos o no, que no tiendan sustancialmente a sustituir a las obras originales en el mercado –con relación al mercado tradicional, razonable y esperado de esas obras– de modo que, de ser permitidos, esos usos destruirían –no que meramente impactarían– los incentivos para la creación.

Reconozco que estas son categorías controversiales y que hay una intensa discusión académica sobre ellas: pero principalmente me refiero a usos que no son comerciales porque, fundamentalmente, carecen de un ánimo de lucro o porque no tienen un impacto sustancial sobre el mercado razonablemente esperado de las obras y sobre los incentivos para crearlas.[36] Por su ambigüedad, la línea entre el uso comercial y el no comercial es normativa y es aquí que nuestras intuiciones sobre (y el peso que le demos a) los paradigmas de *Expresión* y de *Uso personal* harán una diferencia.

---

[36] Este es el debate central en el contexto del cuarto factor del *fair use* estadounidense. *Véase*, por ejemplo, Authors Guild c/ Hathitrust, No. 12-4547-cv (2nd Cir, junio 2014); Authors Guild c/ Google, 954 F.Supp.2d 282 (Nov 14, 2013, S.D.N.Y.); y Bill Graham Archives c/ Dorling Kindersley, 448 F3d 605 de 2006.

En fin, cuando se trate de este tipo de usos no comerciales debe operar un límite importante a la comodificación de las obras y a la lógica del mercado. Ello, pues la comodificación que proviene del *Paradigma de mercado* (en combinación con el de *Propiedad*) impone una visión del usuario-consumidor que ignora al usuario-situado y al usuario-expresivo. Las limitaciones prácticas que el precio impone a los individuos pueden socavar valores políticos importantes.

Hasta ahora he hablado de los derechos de autor como sistema porque refleja y debe reflejar una pluralidad de valores. Pero es un sistema en otro sentido también, pues está compuesto por algo más que leyes: incluye a las tecnologías relevantes, o lo que llamo tecnologías de derechos de autor.

Cuando hablo de tecnología de derechos de autor me refiero a herramientas, instrumentos, máquinas, dispositivos y artefactos; se trate de *hardware* concreto (como elementos de un ISP, CPU, dispositivos móviles, conexiones, satélites y enrutadores de red) o de *software* (sistemas operativos, TCP/IP y aplicaciones) que se emplean para influir en el uso, la distribución o la reproducción de contenido protegido por derechos de autor.

Más concretamente, son aquellas que desempeñan un papel en el acomodo y arreglo de los paradigmas de derechos de autor. Por ejemplo, mecanismos tecnológicos de protección (DRM, por su nombre en inglés) que limitan el uso que podemos dar al contenido, tecnologías de vigilancia y supervisión de contenido por intermediarios (como el *Deep Packet Inspection*), así como las plataformas para compartir y publicar contenido como YouTube o el protocolo de BitTorrent, forman parte de un conjunto tecnológico que incide sobre la relación entre estos paradigmas, a veces con relativa independencia del derecho positivo. Esta “intersección de política y tecnología”, en una continua interacción social valorativamente cargada, es lo que llamo tecnopolítica.[37] Al igual que el derecho de propiedad, la tecnopolítica produce sujetos. En el contexto de mecanismos tecnológicos de protección, por ejemplo, quien rompe esos candados no es sólo un pirata; es a su vez *hacker*.

---

[37] *Véase,* Meléndez Juarbe, Hiram, *supra* nota 2. *Véase también,* Tsekeris, Charalambos, “*Technopolitics”*, *en* Ritzer, George (ed.), *Blackwell Encyclopedia of Sociology,* Hoboken, Blackwell Publishing Inc., 2007.

IV.

Algunos de los espacios –legales y tecnológicos– en que ocurre esta competencia entre paradigmas son conocidos. Menciono algunos para proveer contexto.

Un espacio muy contencioso es el que tiene que ver con la responsabilidad de los intermediarios. Es decir, la posibilidad de hacer responsables a desarrolladores y administradores de tecnologías de derechos de autor, por la potencial infracción de sus clientes y no de la suya directamente.

> La idea de esta estrategia es lograr que estas entidades sientan en su bolsillo presión por el acto potencialmente ilegal de sus clientes y, de esta forma, utilicen sus recursos tecnológicos (así como la oportunidad y superior información que se da en virtud de la relación con sus clientes) para supervisar, castigar o delatar a los usuarios.
> Pero el riesgo principal con esa estrategia es la probabilidad de sobreprotección y el impacto de esta sobre valores vinculados con la libertad de expresión. En la medida en que los intermediarios y los usuarios tienen intereses divergentes, un intermediario no va a tener necesariamente en cuenta el valor expresivo que goza para el usuario la actividad objeto de reglamentación, sino que, racionalmente, va a maximizar su bienestar, buscando reducir el costo esperado de responsabilidad. El problema, en fin, es que al sopesar los costos privados de la responsabilidad frente a sus beneficios –dentro de la concepción racional que constituye su bienestar– el intermediario no considerará los intereses individuales del usuario (o los intereses sociales de que el usuario realice actividad presumiblemente protegida por la libertad de expresión).[38]

El problema, en fin, es que exponer a intermediarios a responsabilidad por actividad potencialmente expresiva de sus clientes, crea poderosos incentivos para eliminar contenido ante la más mínima provocación. Un sistema de derechos de autor que tome en cuenta a los paradigmas de *Expresión* y *Uso personal* evitaría la imposición de regímenes de responsabilidad objetiva a entidades como proveedores de internet o plataformas que viabilizan la comunicación por terceros, como YouTube o Google. También evitaría regímenes que impongan obligaciones vagas y ambiguas que creen incertidumbre y

[38] Meléndez Juarbe, Hiram, "Intermediarios y libertad de expresión: Apuntes para una conversación", en: Bertoni, Eduardo (comp.), *Hacia una Internet libre de censura: Propuestas para América Latina,* Buenos Aires, CELE – Universidad de Palermo, 2012, pp. 109-111.

que, en combinación con el alto costo de litigio y de penalidades, induzcan a los intermediarios a actuar conservadoramente eliminando contenido que, de otro modo, sería legal publicar.[39]

La respuesta más común es ofrecer a los intermediarios una suerte de inmunidad contra demandas, pero condicionada al cumplimiento con ciertas normas. Las condiciones para ganarse esta inmunidad, sin embargo, pueden ser inaceptables. Un ejemplo problemático de este tipo de estructura es el mecanismo de notificación y retirada –o *notice and takedown*– de la sección 512 del *Copyright Act* de los Estados Unidos[40] (una de sus exportaciones más agresivas, según se refleja en tratados de libre comercio en América Latina[41] y que hoy día se intenta incorporar en el Acuerdo Estratégico Transpacífico de Asociación Económica).[42] Aunque hay aspectos del sistema estadounidense que se pueden recomendar, también posee características que gritan reforma precisamente por favorecer el retiro de material casi como un reflejo involuntario tras recibir una notificación privada –aun cuando ella sea de dudosa validez–.

---

39 Véase en esta dirección el fallo CSJN, María Belén Rodríguez c/ Google Inc., R 522 XLIX, del 28 de octubre de 2014.

40 La *Online Copyright Infringement Liability Limitation Act*, 17 U.S.C.A. § 512 (2005 y Supp. 2014), fue aprobada como forma de implementar el Tratado de la OMPI sobre Derecho de Autor de 1996, aunque dicho tratado no requiere esa innovación. Lo que sí contiene es un acuerdo sobre la inmunidad de intermediarios ("*Agreed statements concerning Article 8*: *It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11bis(2).*"). La Unión Europea provee un sistema similar en el Artículo 14 de la Directiva sobre el comercio electrónico, 2000 O.J. (L 178) 1 (E.U.).

41 *Véase,* Ruiz Gallardo, Claudio, y Lara Galvéz, Juan Carlos, "Responsabilidad de los proveedores de servicios de internet (ISPS) en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica", en: Bertoni, Eduardo (comp.), *Hacia una Internet libre de censura: Propuestas para América Latina,* Buenos Aires, CELE – Universidad de Palermo, 2012. *Véase también,* Tratado de Libre Comercio Estados Unidos-Chile, Office of the United States Trade Representative, 2003, disponible en: http://1.usa.gov/1JVvNwp; Tratado de Libre Comercio entre Estados Unidos, República Dominicana y Centroamérica, Office of the United States Trade Representative, 2004, disponible en: http://1.usa.gov/UtCYCI; Acuerdo de Promoción Comercial Estados Unidos-Perú, Office of the United States Trade Representative, 2006, disponible en: http://1.usa.gov/1QEMf3u; Acuerdo de Promociones Comerciales entre Estados Unidos y Colombia, Office of the United States Trade Representative, 2006, disponible en: http://1.usa.gov/1JVw1nm; Tratado de Libre Comercio entre Panamá y Estados Unidos, Office of the United States Trade Representative, 2007, http://1.usa.gov/1nD2q7B.

42 Acuerdo Estratégico Trans-Pacífico de Asociación Económica, WikiLeaks, 13 de noviembre de 2013, disponible en: https://wikileaks.org/tpp-ip2/, *add.* III, Capítulo de [derechos] de propiedad intelectual. Nota del editor: el Acuerdo Estratégico Trans-Pacífico de Asociación Económica fue firmado el 5 de octubre de 2015, posterior a la redacción del presente capítulo.

En cambio, en otros sistemas opera un mecanismo de *notice and notice*, que obliga al intermediario a remitir a sus clientes notificaciones emitidas por los usuarios pero no serán responsables por los actos de terceros ni están obligados a retirar el material por la mera presentación de una notificación.[43] En Chile, por su parte, el sistema requiere intervención judicial antes de obligar a un intermediario el retiro de material.[44] El Artículo 19 del Marco Civil en Brasil incorpora directamente el *Paradigma de expresión* al vislumbrar la responsabilidad de los proveedores de servicio de internet (incluyendo en el contexto de derechos de autor) como un problema de censura, aunque está por verse qué resultará de esto más específicamente.[45] Y, desde luego, el reciente fallo de la Corte Suprema Argentina apunta claramente en esta dirección.[46]

Otra instancia importante es la que tiene que ver con las Medidas Tecnológicas de Protección (MTP) o *Digital Rights Management* (DRM). A partir del Tratado de la OMPI sobre derecho de autor, los Estados firmantes deben proporcionar "protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos"[47]. Es decir, se trata de

---

43 *Véase,* Canada Copyright Act, R.S.C. 1985, c. C-42, s. 47, Arts. 41.15, 41.26. *Véase también,* Geist, Michael, "*Notice and notice in Canada*", disponible en: *http://bit.ly/1KUhBPf.*

44 *Véase,* Ruiz Gallardo, Claudio, y Lara Galvéz, Juan Carlos, *supra* nota 41, pp. 73-81; *Véase también,* Ley Núm. 20435, Mayo 5, 2010, Diario Oficial, Art. 85, Chile.

45 El texto dice: *Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrario. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal... Lei Ordinária 12.965 de 23 de abril de 2014, Diário Oficial da União [D.O.U.] de 24.04.2014, Art. 19 (Brazil).*

46 CSJN, " Rodríguez, María Belén c/ Google, Inc., R 522 XLIX", del 28 de octubre de 2014. Es razonable concluir que la violación de derechos de autor es una de esas instancias que levantan "lesiones (…) de otra naturaleza" que exigen ser deliberadas judicial o administrativamente. *Véase también*, Meléndez Juarbe, Hiram, *supra* nota 38.

47 El tratado de la Organización Mundial de la Propiedad Intelectual sobre derecho de autor, 12 de abril de 1997, S. Treaty Doc. No. 105-17, establece en su artículo 11: "Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley." Para un análisis *véase,* Geist, Michael, "*The Case for Flexibility in*

protecciones legales contra la elusión o *hacking* de tecnologías diseñadas para controlar el uso de las obras en formato digital.

Muchas jurisdicciones han dispuesto –sin que ello sea realmente requerido por ese tratado– mecanismos que prohíben el acto de eludir estas tecnologías independientemente de cualquier reclamo subyacente de derechos de autor.[48] Es decir que, en esas jurisdicciones, constituye una violación el que una persona rompa o eluda medidas tecnológicas de protección –o provea los mecanismos para ello– aun si con ello, quien los elude, no violenta derechos de autor (porque, por ejemplo, el uso constituya *fair use* o la obra esté en el dominio público).[49] Un sistema con estas características permite el control de todas las facetas de uso de una obra, aun en privado y para fines personales y no comerciales. El usuario situado que interese explorar elementos culturales protegidos de esta manera –aun en la intimidad– sólo lo podrá hacer desde la ilegalidad.[50] Este acto lo calificaría como *hacker*.

Una alternativa para dar mayor presencia a los paradigmas de *Expresión* y de *Uso personal*, sería legislando mecanismos como el *fair use* estadounidense (o que los tribunales lo impongan como cuestión constitucional) que, con todos sus problemas, provee una amplia gama de usos no autorizados para fines de parodia, crítica, educativos y otros. El Tribunal Supremo de los EE.UU. ha sugerido que el *fair use* tiene una dimensión constitucional, por virtud de la garantía a la libertad de expresión de la Primera Enmienda.[51] En diferentes grados, casi todos los sistemas, tanto civilistas así como en el *common law*, contienen algún cuerpo de limitaciones y excepciones a los derechos de autor; algunas generales, otras detallando usos específicos permitidos a un menor o mayor grado.[52]

Implementing the WIPO Internet Treaties: An Examination of the Anti-Circumvention Requirements” en: Geist, Michael (ed.), *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda,* Toronto, Irwin Law Inc., 2010.

48 *Véase,* Cohen, Julie, "*A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace”*, en: *Connecticut Law Review,* Vol. 28, Hartford, University of Connecticut School of Law, 1996, pp. 981-1024: *“[T]he civil remedies... are not remedies for copyright infringement, but separate civil penalties tied to the act of “tampering” itself.”*

49 *Véase*, Geist, *supra* nota 47. *Véase también,,* Universal Studios c/ Corley, 273 F.3d 429, 459 (2d Cir. 2001).

50 Exploré algunos elementos de entornos protegidos por MTP en Meléndez Juarbe, Hiram, “*DRM Interoperability”,* en: Boston University Journal of Science & Technology Law, Vol. 15, Boston, Boston University, 2009.

51 *Véase,* Golan c/ Holder, 565 U.S. ___, 132 S.Ct. 873 (2012). *Véase también*, Eldred c/ Ashcroft, *supra* nota 9.

52 *Véase,* Goldstein, Paul, *International Copyright: Principles, Law, and Practice*, Oxford, Oxford University Press, 2012, § 5.5, p. 293.

Habrá que evaluar estas excepciones en cada sistema para ver cómo queda la alineación de paradigmas de derechos de autor. Estos mecanismos de excepción constituyen uno de los pilares más importantes para hacer valer los derechos de libertad de expresión hoy día, ya que la comunicación y la argumentación se dan no sólo con palabras, sino con los comandos de cortar, copiar y pegar.

Canadá, donde los tribunales han expandido recientemente sus disposiciones de *fair dealing*[53], va más lejos al proveer estatutariamente una excepción específica para el *user-generated content* (pensado para *mashups* y demás prácticas no comerciales en redes sociales), de modo que no constituye una violación publicar de buena fe obras de otras personas para fines no comerciales, siempre que se atribuya la autoría correctamente.[54] También se proveen excepciones para el uso personal privado[55] y para realizar copias de resguar-

---

53 Geist, Michael (ed.), *The Copyright Pentalogy: How the Supreme Court of Canada Shook the Foundations of Canadian Copyright Law*, Otawa, University of Otawa Press, 2013.

54 El texto estatutario lee como sigue: *(1) It is not an infringement of copyright for an individual to use an existing work or other subject- matter or copy of one, which has been published or otherwise made available to the public, in the creation of a new work or other subject-matter in which copyright subsists and for the individual –or, with the individual's authorization, a member of their household– to use the new work or other subject-matter or to authorize an intermediary to disseminate it, if (a) the use of, or the authorization to disseminate, the new work or other subject-matter is done solely for non-commercial purposes; (b) the source — and, if given in the source, the name of the author, performer, maker or broadcaster — of the existing work or other subject-matter or copy of it are mentioned, if it is reasonable in the circumstances to do so; (c) the individual had reasonable grounds to believe that the existing work or other subject-matter or copy of it, as the case may be, was not infringing copyright; and (d) the use of, or the authorization to disseminate, the new work or other subject-matter does not have a substantial adverse effect, financial or otherwise, on the exploitation or potential exploitation of the existing work or other subject-matter — or copy of it — or on an existing or potential market for it, including that the new work or other subject-matter is not a substitute for the existing one. (2) The following definitions apply in subsection (1). "intermediary" means a person or entity who regularly provides space or means for works or other subject-matter to be enjoyed by the public. "use" means to do anything that by this Act the owner of the copyright has the sole right to do, other than the right to authorize anything.* Canada Copyright Act, R.S.C. 1985, c. C-42, s. 47, art. 29.21.

55 Sobre este tema, el parlamento canadiense aprobó este texto: *(1) It is not an infringement of copyright for an individual to reproduce a work or other subject-matter or any substantial part of a work or other subject- matter if (a) the copy of the work or other subject-matter from which the reproduction is made is not an infringing copy; (b) the individual legally obtained the copy of the work or other subject-matter from which the reproduction is made, other than by borrowing it or renting it, and owns or is authorized to use the medium or device on which it is reproduced; (c) the individual, in order to make the reproduction, did not circumvent, as defined in section 41, a technological protection measure, as defined in that section, or cause one to be circumvented; (d) the individual does not give the reproduction away; and (e) the reproduction is used only for private purposes. (2) For the purposes of paragraph (1)(b), a "medium or device" includes digital memory in which a work or subject-matter may be stored*

do.[56] Asimismo, el Reino Unido recientemente inauguró unas excepciones más limitadas para realizar copias personales no comerciales, para fines de resguardo (incluyendo en la nube) y para cambio de formato. Estas disposiciones permiten que un individuo transfiera su copia a un tercero (sin fines comerciales) siempre que destruya su copia.[57] Aun así, este tipo de excepción particular para uso no comercial personal podría ser de muy limitado alcance si no viene acompañada de excepciones generales para contextos variados.

Mercado, *Propiedad*, *Expresión* y *Uso personal*. En todos estos ejemplos, diversos sistemas de derechos de autor definen la fuerza relativa de cada una de estas visiones de mundo. La pregunta que tenemos sobre la mesa es: ¿cuál es el arreglo que vamos a preferir? Cada país tendrá su propia forma de estructurarlos. Pero de lo que no me cabe duda es que los valores detrás de la expresión y el uso Personal deben, como cuestión normativa y política, ejercer fuerza de gravedad en esta constelación de valores que llamamos un sistema de derechos de autor.

---

for the purpose of allowing the telecommunication of the work or other subject-matter through the Internet or other digital network. (3) In the case of a work or other subject-matter that is a musical work embodied in a sound recording, a performer's performance of a musical work embodied in a sound recording or a sound recording in which a musical work or a performer's performance of a musical work is embodied, subsection (1) does not apply if the reproduction is made onto an audio recording medium as defined in section 79. (4) Subsection (1) does not apply if the individual gives away, rents or sells the copy of the work or other subject-matter from which the reproduction is made without first destroying all reproductions of that copy that the individual has made under that subsection. Ibíd., Art. 29.22

56 El artículo de la ley canadiense dice lo siguiente: (1) *It is not an infringement of copyright in a work or other subject-matter for a person who owns — or has a licence to use — a copy of the work or subject- matter (in this section referred to as the "source copy") to reproduce the source copy if (a) the person does so solely for backup purposes in case the source copy is lost, damaged or otherwise rendered unusable; (b) the source copy is not an infringing copy; (c) the person, in order to make the reproduction, did not circumvent, as defined in section 41, a technological protection meas- ure, as defined in that section, or cause one to be circumvented; and (d) the person does not give any of the reproductions away. (2) If the source copy is lost, damaged or otherwise rendered unusable, one of the reproductions made under subsection (1) becomes the source copy. (3) The person shall immediately destroy all reproductions made under subsection (1) after the person ceases to own, or to have a license to use, the source copy. Ibíd.*, Art. 29.24.

57 Las regulaciones británicas parecen reconocer una "*first sale*" o agotamiento digital: *(8) Copyright in a work is also infringed if an individual, having made a personal copy of the work, transfers the individual's own copy of the work to another person (otherwise than on a private and temporary basis) and, after that transfer and without the licence of the copyright owner, retains any personal copy. The Copyright and Rights in Performances (Personal Copies for Private Use) Regulations 2014, SI 2014/2361 (U.K.).*

V.

Diego Gómez, un estudiante de doctorado colombiano, subió al Internet una tesis de maestría de otra persona para compartirla con colegas científicos. Como consecuencia, Diego se enfrenta a una posible condena de hasta ocho años de cárcel por hacer lo que hacen todos los científicos que merezcan ser identificados como tal: compartir el conocimiento.[58]

Desconozco si este tipo de situación es común en ese país o en la región. Pero no puede dudarse que un sistema mejor balanceado hubiese impuesto requisitos de acceso abierto a la investigación auspiciada con fondos públicos, como se hace en Argentina.[59] Quizás en ese caso, Diego no hubiese tenido la necesidad de compartir algo ya disponible a todos. Tal vez un sistema más equilibrado reconocería amplias excepciones para el uso personal de obras protegidas por derecho de autor. O, tal vez, facilitaría mecanismos para que el autor objete la distribución de contenido sin que esté en juego la libertad personal ni la libertad de expresión. En todo caso, en el caso de Diego parece haber un desplazamiento absoluto de los paradigmas de *Expresión* y de *Uso personal*, por los de *Mercado* y de *Propiedad*.

El caso de Diego Gómez es, como señala la Fundación Karisma de Colombia, "absurdo"[60]. Es también trágico, porque independientemente de su resultado, la mera amenaza de privar al individuo de la libertad probablemente tendrá un efecto disuasivo sobre una conducta que contribuye enormemente a un entorno expresivo saludable.

---

58 *Véase,* Fundación Karisma, "Fundación Karisma apoya a Diego Gómez y se suma a la campaña #CompartirNoEsDelito", disponible en: http://bit.ly/1QXxj2u; Cerda Silva, Alberto J., "*Derechos humanos y delitos contra la propiedad intelectual"*, disponible en: http://bit.ly/205ZMDP; Kloc, Joe, "*Colombian Student Facing Prison for Sharing Research Paper Online"*, en: Newsweek, 7 de agosto de 2014, disponible en: http://bit.ly/23GVxmF; Gómez, Diego, "R*ead My Story"*, disponible en: http://bit.ly/1t3w46e.

59 *Véase*, Ley No. 26 899, Sistema nacional de ciencia, tecnología e innovación. Repositorios digitales institucionales de acceso abierto, B.O., Argentina, 13 de noviembre de 2013. Esta ley tiene sus propios problemas. Por ejemplo, no queda claro en qué consiste el acceso abierto allí dispuesto (si, por ejemplo, sólo se trata de acceso gratis o si, en cambio, incluye acceso libre); y también crea imprecisión en torno al momento en que se activa la obligación de colocar investigación en repositorios (si es seis meses luego de la aceptación o de la publicación de un artículo, momentos que pueden estar apartados sustancialmente en el tiempo). Además la ley sólo aplica a publicaciones de índole científica o técnica, ignorando la producción intelectual en las ciencias sociales o humanidades, también financiada por el Estado. *Véase también*, Suber, Peter, *Open Access,* Cambridge, MIT Press, 2012, disponible en: http://bit.ly/1zqZBYx.

60 *Véase,* Fundación Karisma, *supra* nota 58.

Desde un punto de vista que enfatiza los intereses más amplios de un Estado democrático, este tipo de casos absurdos revela otro tipo de problema. Y es que el poder público debe ejercerse legítimamente. Esta legitimidad depende, entre muchas otras cosas, de que la población cuya libertad es estructurada y limitada por el derecho conciba a la norma jurídica que le rige como razonable, y no despótica y estúpida. Pero cuando los ciudadanos se enfrentan a un potencial castigo que, con muy buena razón, se piensa es "absurdo", arbitrario y caprichoso, se amenaza la legitimidad de ese sistema.[61] ¿Qué vamos a decir de la legitimidad de un Estado de derecho que criminaliza prácticas cotidianas y masivamente adoptadas por la población? Estas prácticas emergen del amor por el conocimiento, la búsqueda de la verdad y del poderoso deseo de vivir en una comunidad de seres interrelacionados. La construcción del sujeto como un criminal, un pirata, en casos como éstos parece contraproducente desde esta perspectiva.

En el contexto colombiano, muy valiosos compañeros y compañeras han levantado su voz. Se trata de queridos colegas en toda América Latina y el Caribe, colaborando en una hermosa y revoltosa conspiración para construir una sociedad libre, abierta, democrática y amante de la búsqueda del conocimiento que sea, a su vez, respetuosa de los intereses de los creadores. Al final, está de parte nuestra, la sociedad civil, –con nuestras acciones, demandas y, sobre todo, nuestra palabra–, exigir a nuestros conciudadanos, operadores políticos, tribunales y parlamentos que, cuestionen el tipo de sistema de autor que tenemos. Y, en ese ejercicio, está de parte nuestra cuestionarnos en voz alta y en el debate público, ¿qué sistema de derechos de autor queremos?, ¿para qué lo queremos? y ¿qué valores deseamos que refleje?

61 Fontánez Torres, Érika, y Meléndez Juarbe, Hiram, "Derecho al Derecho: Una Apuesta por la Democratización Radical de lo Jurídico", en: *Revista Jurídica Digital de la Universidad de Puerto Rico,* No. 83, San Juan, UPR, 2014, disponible en: http://bit.ly/1P39uUh.

El uso de la DMCA para limitar la libertad de expresión [1]

Eduardo Bertoni y Sophia Sadinsky[2]

Resumen

Este artículo analiza el uso indebido de la Ley de Derechos de Autor del Milenio Digital de Estados Unidos *(Digital Millennium Copyright Act,* DMCA) para censurar el discurso político y otras expresiones en línea, con atención especial a su impacto en América Latina. Para ello, se revisan las características y el alcance de la DMCA y se resaltan diversos casos en América del Norte y América del Sur en los cuales se ha usado esta legislación para eliminar contenido en línea. El documento resume brevemente los estándares internacionales y regionales que regulan la libertad de expresión y cómo el uso abusivo de la DMCA viola dichas normas. Por último, presenta las propuestas vigentes que buscan mitigar el uso de la DMCA para censurar la expresión protegida y ofrece recomendaciones adicionales.

I. Introducción

El 9 de octubre de 2013 el cineasta ecuatoriano Pocho Álvarez advirtió que uno de sus documentales había sido quitado de su página de YouTube.

---

[1] Este documento fue elaborado por Eduardo Bertoni, director del del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, y Sophia Sadinsky, becaria del programa Princeton in Latin America en el CELE.

[2] Este artículo fue publicado originalmente en inglés en la Revista de *Derecho, Comunicaciones y Nuevas Tecnologías*, No. 13, enero - junio de 2015, ISSN 1909-7786, Facultad de Derecho, Universidad de los Andes, Colombia, disponible en: http://bit.ly/1JVwO7G. Tradución al español por Gabriela Haymes.

En vez del documental, se visualizaba un mensaje de YouTube que le avisaba que el video ya no estaba disponible debido a violación de derechos de autor. El documental, titulado *Acoso a Intag*, describe brevemente el hostigamiento sufrido por la comunidad indígena Intag debido a su oposición a la minería en la región. El video contenía menos de 20 segundos de imágenes y grabaciones de audio con la voz del Presidente de Ecuador Rafael Correa, durante los cuales se repetía la frase "veamos quiénes son los que están causando estos problemas", que sugería que comunidades locales eran las responsables de frenar el desarrollo de la región. La remoción del video se justificó alegando que Álvarez había infringido las normas sobre derechos de autor al usar secuencias de una grabación del presidente Correa tomadas de su programa semanal que se transmite a todo el país[3].

En este caso, las directrices sobre derechos de autor relevantes eran las establecidas por la Ley de Derechos de Autor del Milenio Digital (*Digital Millennium Copyright Act*, DMCA), sancionada por el Congreso de Estados Unidos en 1998 para combatir las violaciones de este derecho en línea. La Ley contempla un sistema abreviado de "notificación y cancelación", que permite a los titulares de derechos solicitar a proveedores de servicios en línea, como sitios web de medios sociales, que quiten contenidos o enlaces invocando la violación de derechos de autor, sin ningún tipo de supervisión judicial. Mientras cumplan con estas solicitudes, las empresas como YouTube podrán eludir la responsabilidad por el contenido que publiquen sus usuarios.

Al igual que en el caso de Álvarez, esto implica que el contenido impugnado casi siempre se retira inmediatamente, aunque los usuarios pueden apelar estas cancelaciones, y para ello a menudo invocan el principio de "uso justo" (*fair use*), una excepción contemplada por el derecho estadounidense que permite reproducir materiales sujetos a propiedad intelectual para determinados fines como crítica, comentarios, parodias, enseñanza e investigación. Cuando se inicia un proceso de contestación, el contenido se repone generalmente en el término de dos semanas; sin embargo, para entonces la cancelación ya ha tenido consecuencias significativas, particularmente en el caso de las expresiones políticas. La DMCA se utiliza con frecuencia para lograr que se quiten contenidos en momentos políticos decisivos, o en medio de períodos de campaña, y silenciar así a voces opositoras justamente cuando estas son más indispensables.

---

3 Algunos de estos sucesos fueron documentados en el artículo de opinión Bertoni, E., y Vivanco, J.M. "La censura en Ecuador llegó a Internet", *El País*, 12 de diciembre de 2014, disponible en: http://bit.ly/1BJN0QC.

El uso de la DMCA como herramienta de censura política no está asociada con ninguna región ni ideología específica. El presente informe muestra que ha sido aplicada en una amplia variedad de casos, en distintas regiones del mundo, que difieren sustancialmente en cuanto a su alcance, contenido y los actores implicados. Por último, considera opciones viables para prevenir abusos de la DMCA en el futuro. Numerosos activistas, especialistas en derecho, representantes de la sociedad civil e incluso proveedores de servicios en línea han planteado distintas formas de abordar esta consecuencia de la DMCA, que muchos califican de nociva y que no habría sido buscada por sus autores. Algunos reclaman una revisión total de la Ley, mientras que otros recomiendan implementar cambios concretos en su aplicación para resguardar los derechos de libertad de expresión de los usuarios. Este informe ofrece una reseña de las violaciones de derechos que se producen como resultado de abusos de la DMCA, y un análisis equilibrado de las ventajas a largo plazo y las posibles fallas en las recomendaciones que se han formulado sobre la materia.

II. La DMCA: análisis general y uso indebido de las directrices sobre derechos de autor

La sanción en 1998 de la DMCA fue la conclusión de una iniciativa de los legisladores por actualizar la normativa estadounidense de derechos de autor para que reflejara el cambiante panorama digital. La disposición de la Ley sobre "notificación y cancelación" abreviada procura proteger a los proveedores de servicios en línea frente a una eventual responsabilidad excesiva. Así, se concede a proveedores como Google o Twitter una protección, conocida como "puerto seguro" (*safe harbor*), frente a multas por contenidos que infringen derechos de autor, a cambio de que los retiren rápidamente, sin que medie ninguna acción legal ni control judicial.

Muchos activistas y expertos de Internet coinciden en que la DMCA ha posibilitado la veloz expansión de Internet, al reafirmar la importancia de un sistema de notificación y cancelación que no solo protege la propiedad intelectual en línea, sino que además otorga a proveedores de servicios un nivel de inmunidad que ha demostrado ser crucial para la innovación en línea.[4] Es

[4] *Véase,* Edwards, Lilian, "*The role and responsibility of internet intermediaries in the field of copyright and related rights",* en: *WIPO,* 2011, disponible en: http://bit.ly/1KUiYx9; Electronic Frontier Foundation, *"Digital Millennium Copyright Act",* disponible en: http://bit.ly/1VH03vs; Kravets, David, "*10 years later, misunderstood DMCA is the law that saved the web",* 27 de octubre de 2008, en: *Wired*, disponible en: http://bit.ly/2060Ozx; Stallman, Erik,

fácil pensar situaciones que dan testimonio del valor que reviste un sistema de este tipo para empresas y usuarios por igual; basta con imaginar cuáles serían las consecuencias para la participación cívica si los usuarios tuvieran que justificar su titularidad sobre contenidos o sus derechos de uso justo antes de subir cualquier material a la red. Asimismo, el libre flujo de contenidos se vería obstaculizado si un proveedor como YouTube tuviera que corroborar la titularidad antes de admitir cada uno de los miles de millones de videos que aloja. El sistema de notificación y cancelación ha conseguido eludir estos inconvenientes, creando un mecanismo sencillo para proteger los derechos de autor, sin frenar el ritmo vertiginoso de las publicaciones digitales.

Sin embargo, también ha abierto la posibilidad de violaciones indiscriminadas a la libertad de expresión. La facilidad con la cual se pueden emitir pedidos de cancelación, y los incentivos para que las empresas respondan favorablemente y con rapidez, han dejado un amplio margen para que titulares de derechos de autor intercedan de manera abusiva e insistente, exigiendo la cancelación de contenidos que no consideran convenientes. La disposición no exige que intermediarios, como YouTube y Facebook, examinen la validez de las peticiones antes de quitar el contenido violatorio, sino que proceden a quitar inmediatamente el material cuestionado, a menudo tras constatar únicamente los datos de contacto de la parte que objetó el contenido. A su vez, numerosos proveedores de servicios han adoptado alguna variante de la política de "tres infracciones" (*three strikes*), y cierran las cuentas de los usuarios una vez que han debido realizar una cierta cantidad de cancelaciones. Si bien en general los usuarios apelan estas cancelaciones invocando el principio de "uso justo"[5], el proceso de restablecimiento lleva hasta dos semanas, lo cual puede representar una demora decisiva en relación con sucesos políticos y acciones de activismo en las cuales la oportunidad es clave.

"*Exporting the DMCA",* en: *Center for Democracy & Technology Blog*, 17 de octubre de 2014, disponible en: http://bit.ly/1nKy7wu. .

5 El académico y experto en Internet Lawrence Lessig ha destacado las dificultades que supone depender del "uso justo" como una solución única para proteger contenidos que no resultan violatorios, y ha señalado al respecto que las tecnologías digitales han cambiado el modo en que se usan los contenidos y las libertades asociadas. Según advierte, las estructuras legales existentes no se han puesto al día con el mundo digital, y han delegado en gran medida en el principio de "uso justo" la protección de una amplia variedad de obras creativas, que anteriormente se encontraban tuteladas como "usos libres" que no conllevaban la afectación de derechos de autor. Para obtener más información, *véase,* Lessig, Lawrence, "*CC in Review: Lawrence Lessig on CC & fair use",* Creative Commons, 26 de octubre de 2005, disponible en: http://bit.ly/1PwKXIJ.

III. Ejemplos de casos de América del Norte

El uso abusivo de la DMCA fue habitual durante las elecciones presidenciales de 2008 en Estados Unidos, y los dos principales partidos políticos se vieron afectados por la cancelación de contenidos que limitó la libertad de expresión durante sus campañas. En septiembre de ese año, por ejemplo, NBC solicitó la cancelación de un video satírico de la campaña de Obama. El video viral contenía una grabación de archivo del periodista Tom Brokaw, en la cual anunciaba que el senador John McCain había "ganado", y tenía como propósito instar a quienes simpatizaban con Obama a que se acercaran a las urnas. El video fue dado de baja de YouTube luego de que NBC planteara que el anuncio era violatorio de contenidos protegidos por derechos de autor que pertenecían a esta cadena, apenas días antes del vencimiento del plazo para que los votantes se inscribieran en el padrón electoral.[6]

A su vez, al mes siguiente le tocó al equipo de campaña de McCain ser objeto de acciones por violaciones de derechos autor, planteadas en este caso por otra emisora, CBS News, que cursó un aviso de cancelación de contenidos como reacción a la difusión de un video de la campaña de McCain[7]. La intención del anuncio era poner en evidencia la actitud sexista contra Sarah Palin, y mostraba a la presentadora de CBS Katie Couric diciendo: "Una de las grandes enseñanzas de la campaña es el rol persistente y aceptado del sexismo en la vida de los estadounidenses"[8]. En el video original, que se difundió meses antes de que Palin se lanzara a la carrera electoral, Couric se refería en realidad al caso de Hillary Clinton. La campaña McCain-Palin sufrió varias cancelaciones de contenidos por parte de distintos medios a lo largo del período electoral, incluidos Fox News y Christian Broadcasting Network, y por ello, en octubre de 2008, enviaron una carta a YouTube, en la cual enumeraban los "excesivos reclamos por derechos de autor" dirigidos a expresiones políticas que "se encontraban claramente protegidas por la doctrina del uso justo"[9].

En Estados Unidos ha persistido el uso abusivo de la DMCA por ambos partidos para acallar expresiones políticas, y no solo durante los períodos de

---

6 *Véase,* Electronic Frontier Foundation, "*NBC issues takedown on viral Obama ad",* en: *EFF*, 2008, disponible en: http://bit.ly/1SVR8bC.

7 *Véase,* Electronic Frontier Foundation, "*CBS News censors McCain ad during heated presidential campaign", EFF*, 2008, disponible en: http://bit.ly/1UGroxS.

8 Smith, Ben, "*CBS takes down McCain web ad, suggests it's 'misleading'",* en: *Politico*, 10 de septiembre de 2008, disponible en: http://politi.co/1UGrs0q.

9 Von Lohmann, Fred, "*McCain Campaign Feels DMCA Sting",* en: *Electronic Frontier Foundation Deeplinks Blog*, 14 de octubre de 2008, disponible en: http://bit.ly/1PwLjzf.

campaña. En 2009, la National Organization for Marriage, una agrupación antigay que se opone al matrimonio entre personas del mismo sexo, produjo un anuncio en el cual se mostraba a varios actores supuestamente atemorizados ante la posibilidad de que se reconociera igualdad de derechos para las parejas gay. Posteriormente, otra organización encontró y difundió en línea un video de las "audiciones" que se llevaron a cabo para la publicidad, y Rachel Maddow de MSNBC mostró estas grabaciones en su programa de televisión, burlándose de la falta de credibilidad del anuncio y criticando su peligroso mensaje. La National Organization for Marriage envió una advertencia a YouTube al amparo de la DMCA, aseverando que las grabaciones de la audición eran contenidos sujetos a derechos de autor, y debido a ello el programa de Maddow fue quitado de YouTube[10].

Otro caso con fuertes implicancias políticas ha sido el de Right Wing Watch (RWW), un proyecto de la organización People for the American Way que da seguimiento y difusión a las actividades de figuras de sectores de derecha en el ámbito de la religión y la política. En 2013, Gordon Klingenschmitt, un capellán de la Marina que actualmente integra la Cámara de Representantes de Colorado, cursó a YouTube diversas notificaciones conforme a la DMCA para la cancelación de una serie de videos -que estaban claramente alcanzados por la excepción de uso justo- del canal de RWW, donde se mostraban polémicas declaraciones efectuadas por grupos y personas de adscripción conservadora. Entre estos videos había varios segmentos tomados del propio programa de Klingenschmitt, denominado *Pray in Jesus' Name* (Reza en nombre de Jesús), que también se transmite por YouTube. Aunque los videos posteriormente se restablecieron luego de que RWW planteara un recurso de contestación, la embestida de Klingenschmitt logró igualmente que los contenidos en la cuenta de RWW se dieran de baja dos veces[11].

Si bien en la campaña presidencial de 2012 las cancelaciones posibilitadas por la DMCA fueron menos comunes, las elecciones legislativas de mitad de período en 2014 fueron escenario de numerosas violaciones de la libertad de expresión fundadas en la DMCA. En octubre, la junta editorial del periódico de Kentucky *Courier-Journal* entrevistó a Alison Lundergan Grimes, candidata demócrata al Senado. La entrevista, que se transmitió en vivo y posteriormente

10 Véase, Poulsen, Kevin, "*Anti-gay-rights group gets MSNBC clip pulled from YouTube",* en: *Wired*, 13 de abril de 2009, disponible en: *http://bit.ly/1Pdvg5C*.

11 Véase, McSherry, Corynne, "*No more downtime for free speech: EFF helps People for the American Way challenge DMCA abuser",* en: *Electronic Frontier Foundation Deeplinks Blog,* 8 de diciembre de 2013, disponible en: http://bit.ly/IBrrfi.

fue publicada en Internet por un crítico, contenía 40 segundos en los cuales Grimes se negaba admitir si había votado por el presidente Obama, quien no goza de popularidad en su Estado[12]. Gannett Co. Inc., un grupo de medios que es propietario de *Courier-Journal*, presentó un reclamo por derechos de autor ante YouTube y consiguió que el video de la entrevista se quitara rápidamente[13].

Estados Unidos no es el único país que apela al uso de la DMCA como mecanismo para silenciar comentarios políticos y sociales. En 2013, la oficina de turismo de Alberta, en Canadá, emitió un aviso de cancelación de contenidos para que se quitara un video producido por dos comediantes en el cual se parodiaba una publicidad de promoción turística de Alberta. En el video se usan unos pocos segundos de la publicidad de la oficina de turismo, y se contrastan las imágenes de entornos naturales de la región mostrados en el anuncio con la degradación ambiental que estaba ocurriendo en los yacimientos petrolíferos en Alberta. El video cita a modo de eufemismo el eslogan de la oficina de turismo: “Recuerde respirar”. Tras su difusión, la oficina de turismo contrató a un estudio de abogados -que también representa a una de las principales empresas petroleras de la región- para que tramitara la cancelación del video, al amparo de la DMCA, ante YouTube, y este finalmente fue retirado.[14]

En otro caso canadiense, el Correo de Canadá planteó una solicitud de cancelación a YouTube, luego de que miembros de un sindicato publicaran un video en el cual se mofaban de su Directora Ejecutiva, Moya Greene. El video, titulado “*The Greench*”, se publicó en medio de acaloradas disputas por el pago de licencias por enfermedad, y adaptaba la letra de la conocida canción de Dr. Seuss, “*You’re a mean one, Mr. Grinch”* (“Es usted malvado, Sr. Grinch”), parodiando a la Directora Ejecutiva y sus políticas corporativas. El aviso infundado de cancelación emitido por la empresa, y como resultado del cual se quitó el video de YouTube, indicaba que se habían violado derechos de autor debido a que en el video se mostraba fugazmente una fotografía retocada de la Directora Ejecutiva[15].

---

12 Véase, Bump, Phillip, “40 painful seconds of Alison Lundergan Grimes refusing to say whether she voted for President Obama”, en: Washington Post, 9 de octubre de 2014, disponible en: http://wapo.st/1vRRVMb.

13 Véase, McSherry, Corynne, “For shame: Gannett abuses DMCA to take down political speech”, en: *Electronic Frontier Foundation Deeplinks Blog,* 10 de octubre de 2014, disponible en: http://bit.ly/ZBLX7N.

14 Véase, Stoltz, Mitch, “*Using copyright to silence oil sands satire? How* crude”, en: *Electronic Frontier Foundation Deeplinks Blog*, 20 de agosto de 2013, disponible en: http://bit.ly/1PSoubc.

15 Véase, Masnick, Mike, “*Once again, you don't get to use DMCA takedowns to remove any content you don't like”,* en: *Techdirt,* 30 de enero de 2009, disponible en: http://bit.ly/20mFfQK.

IV. La DMCA en América Latina: casos regionales y contexto

Si bien la Ley de Derechos de Autor del Milenio Digital es una norma estadounidense, la aplicación expansiva que ha tenido resulta llamativa. En parte debido a que la mayoría de los principales medios sociales y motores de búsqueda están alojados en Estados Unidos, la DMCA se ha convertido en la herramienta de referencia automática en las controversias por derechos de autor que tienen lugar en una gran cantidad de países de distintas regiones del mundo, incluida América Latina. El país latinoamericano sobre el cual se tienen mayores registros de uso de la DMCA para censurar expresiones en línea es Ecuador, si bien han empezado a darse casos también en otros países, como Colombia y Brasil. Los casos ecuatorianos se plantearon contra una variedad de usuarios y contenidos, desde productores de documentales que retrataban el activismo de grupos indígenas, hasta usuarios de Twitter que difundían caricaturas sobre acontecimientos políticos a modo de sátira.

En septiembre de 2014, por ejemplo, el administrador de una popular página de Facebook advirtió que el enlace a un video subido anteriormente había sido quitado por violación de derechos de autor. El video, filmado durante la represión violenta de manifestantes estudiantiles ocurrida ese mismo mes, mostraba abusos policiales presuntamente cometidos durante las protestas y contenía secuencias del presidente Correa en las cuales elogiaba la actuación de la Policía. Una semana después, el video además fue quitado de YouTube.

También un documental del cineasta Santiago Villa que criticaba al gobierno de Correa fue sacado de Internet en 2014, tras un aviso de cancelación que alegaba que se utilizaban "imágenes no autorizadas" de la cadena que emite semanalmente Correa. Más tarde ese año, la cuenta de Twitter de Diana Amores, una traductora que habitualmente comparte tuits de contenido humorístico con sus seguidores, fue suspendida luego de que en más de una ocasión Twitter eliminara imágenes que había difundido por este medio, incluidas varias caricaturas. Los reclamos por derechos de autor que consiguieron quitar las imágenes de Amores, y finalmente suspender su cuenta, fueron impulsados por el canal público de televisión EcuadorTV y el partido gobernante Movimiento Alianza País. La infracción a los derechos de autor en la cual estuvo implicada fue absolutamente intrascendente, y consistió en subir una fotografía que mostraba al político en cuestión con una camiseta con el logotipo del partido. Probablemente el contenido habría sido cuestionado debido al mensaje humorístico que Amores tuiteó con la imagen.

Esta serie desconcertante de cancelaciones efectuadas al amparo de la DMCA tienen un elemento común: instituciones y funcionarios públicos que son hostiles a críticas y parodias. Hay en Ecuador antecedentes de censura durante el período de Correa, quien varias veces se ha extralimitado en sus facultades legislativas como reacción ante opiniones disientes y a menudo ha apelado a leyes penales sobre calumnias para silenciar a opositores. Desde que asumió en 2007, ha intentado que se dicten penas de prisión desorbitantes y se impongan indemnizaciones por varios millones de dólares a medios de comunicación por injurias, y ha demostrado no tener tolerancia alguna con voces disidentes. En 2013, la Asamblea Nacional de Ecuador aprobó una Ley Orgánica de Comunicación que otorga amplia discrecionalidad al gobierno para censurar información pública y juzgar penalmente a periodistas. El gobierno también ha criticado enérgicamente a la Relatoría sobre Libertad de Expresión de la Organización de los Estados Americanos y ha impulsado medidas que limitarían gravemente su autonomía y eficacia en la defensa de la libertad de expresión.

Si bien Ecuador utiliza la DMCA mucho más asiduamente que otros países para disuadir la libre expresión, la práctica se está extendiendo fuera de dicho país. En Colombia, la Iglesia de Dios Ministerial de Jesucristo Internacional, vinculada con el partido colombiano MIRA, ha procurado reiteradamente que se retiren de YouTube videos en los cuales se muestran, por ejemplo, declaraciones efectuadas por el fundador de esa iglesia. Uno de los videos, que fue bloqueado por YouTube a pedido de la iglesia, incluso contenía en el título la aclaración de que se trataba de una parodia.[16]

En Brasil, la DMCA se aplicó para quitar videos en los cuales se criticaba al ex gobernador Aécio Neves, quien fue candidato a presidente en 2014. Si bien no se ha confirmado la identidad del solicitante, muchos creen que sería el mismo Neves el causante de las cancelaciones.[17]

---

16 Véase, Fundación para la Libertad de Prensa, "Iglesia de María Luisa Piraquive bloquea contenidos periodísticos en YouTube*"*, en: *FLIP*, 5 de febrero de 2014, disponible en: http://bit.ly/1ypWJxg.

17 Véase, Sutton, Maira, "*Copyright Law as a Tool for State Censorship of the Internet",* en: *Electronic Frontier Foundation Deeplinks Blog,* 3 de diciembre de 2014, disponible en: http://bit.ly/1rVSJmg.

V. Estándares internacionales sobre censura y libertad de expresión en línea

El uso de la DMCA para suprimir expresiones de ciudadanos no solo es una interpretación lamentable de la protección de los derechos de autor, sino que además contraviene abiertamente los estándares internacionales relativos al derecho de libertad de expresión. Cada uno de los casos antes mencionados está alcanzado por la protección de las directrices de Naciones Unidas y, a nivel regional, por los principios establecidos en el sistema interamericano. El sistema europeo de derechos humanos también contempla parámetros claros para el ejercicio de la libertad de expresión cuya consideración resulta útil, incluso en casos como estos, que no se encuentran alcanzados por la competencia del Tribunal Europeo.

En esta sección se presentan brevemente las normas universales y regionales, además de interpretaciones relevantes sobre su aplicación. No se pretende aquí ofrecer un análisis exhaustivo de los estándares aplicables a la libertad de expresión ni de la jurisprudencia sobre el tema, sino reseñar brevemente las normas pertinentes y ofrecer un breve análisis de las interpretaciones que orientan su aplicación.

1. Estándares de Naciones Unidas

En el sistema de las Naciones Unidas, la libertad de expresión se encuentra reconocida por el artículo 19 de la Declaración Universal de Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), además de otras garantías.

El artículo 19 de la Declaración Universal de Derechos Humanos estipula: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión"[18].

---

18 Asamblea General de las Naciones Unidas, *Declaración Universal de Derechos Humanos*, Resolución A.G. 217 (III), U.N. Doc. A/RES/217(III), 10 de diciembre de 1948, artículo 19, disponible en: http://bit.ly/1hHDu9u.

El artículo 19 del PIDCP establece[19]:

1. Nadie podrá ser molestado a causa de sus opiniones.
2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
   (a) Asegurar el respeto a los derechos o a la reputación de los demás;
   (b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

En su interpretación del artículo 19 del PIDCP, la Observación General N.º 34 del Comité de Derechos Humanos de las Naciones Unidas ratifica que los Estados Parte "tienen la obligación de asegurarse de que su legislación interna haga efectivos los derechos conferidos en el artículo 19 del Pacto", que abarca expresamente "el pensamiento político, los comentarios sobre los asuntos propios y los públicos, las campañas puerta a puerta, la discusión sobre derechos humanos, el periodismo, la expresión cultural y artística, la enseñanza y el pensamiento religioso". Se encuentran protegidas todas las formas de expresión, incluidos "modos de expresión audiovisuales, electrónicos o de Internet, en todas sus formas".

La Observación indica los supuestos excepcionales en los cuales se admiten restricciones a la libertad de expresión, y destaca que las "restricciones deben ser 'necesarias' para la consecución de un propósito legítimo" y "no deben ser excesivamente amplias". Se indica claramente que "el Pacto atribuye una gran importancia a la expresión sin inhibiciones en el debate público sobre figuras del ámbito público y político en una sociedad democrática". El Comité concluye que el Pacto no autoriza "las prohibiciones penales de la expresión de opiniones erróneas o interpretaciones incorrectas de

[19] Asamblea General de las Naciones Unidas, *Pacto Internacional de Derechos Civiles y Políticos*, Resolución A.G. 2200 A (XXI), 999 U.N.T.S. 171, 6 de diciembre de 1966 (en vigor desde el 23 de marzo de 1976).

acontecimientos pasados. No deben imponerse nunca restricciones al derecho a la libertad de opinión".[20]

Ninguna de las dos áreas de restricción se aplica a los casos expuestos en este informe. Por ende, el uso de la DMCA para censurar contenidos en línea en estos casos importa una violación del derecho de libertad de expresión, de conformidad con los estándares establecidos por las Naciones Unidas.

2. Sistema interamericano de derechos humanos

En el sistema interamericano la libertad de expresión se encuentra protegida principalmente por el artículo 4 de la Declaración Americana de los Derechos y Deberes del Hombre y el artículo 13 de la Convención Americana sobre Derechos Humanos[21].

El artículo 4 estipula[22]: "Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio."

El artículo 13 dispone[23]:

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: (a) el respeto a los derechos o a la reputación de los demás; o (b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

---

20 Comité de Derechos Humanos, *Observación General, N.º 34: Artículo 19: Libertad de opinión y libertad de expresión,* 11, Doc. de la ONU CCPR/C/GC/34, 21 de julio de 2011.

21 Si bien Estados Unidos no ha ratificado la Convención Americana sobre Derechos Humanos, la interpretación de este pacto por la Corte Interamericana de Derechos Humanos ha sido importante para dirimir casos sobre libertad de expresión en dicho país.

22 Organización de los Estados Americanos, *Declaración Americana de los Derechos y Deberes del Hombre,* OEA/Ser.L./V.II.23, doc. 21, rev. 6, 1948.

23 Organización de los Estados Americanos, *Convención Americana sobre Derechos Humanos*, O.A.S.T.S.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

La Corte Interamericana de Derechos Humanos ha interpretado en particular el artículo 13, en numerosos casos que deberían ser tomados en cuenta al considerar los estándares que determinan el derecho de libertad de expresión.[24] La Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, en el Marco Jurídico Interamericano

24 La colegiatura obligatoria de periodistas prescrita por ley para la práctica periodística. *Véase, Opinión Consultiva OC-5/85,* 13 de noviembre de 1985, Serie A, N.º 5, ¶ 70.; Corte I.D.H., "Caso Ivcher Bronstein c/ Perú, Interpretación de la Sentencia de Fondo", sentencia del 4 de septiembre de 2001, Serie C No. 84; Corte I.D.H., "Caso Herrera Ulloa c/ Costa Rica, Excepciones preliminares, Fondo, Reparaciones y Costas", sentencia del 2 de julio de 2004, Serie C N.º 107; Corte I.D.H., "Caso Ricardo Canese c/ Paraguay, Fondo, Reparaciones y Costas", sentencia del 31 de agosto de 2004, Serie C No. 111; Corte I.D.H., "Caso Palamara Iribarne c/ Chile, Fondo, Reparaciones y Costas", sentencia del 22 de noviembre de 2005, Serie C N.º 135; Corte I.D.H., "Caso Claude Reyes y otros c/ Chile, Fondo, Reparaciones y Costas", sentencia del 19 de septiembre de 2006, Serie C N.º 151; Corte I.D.H., "Caso Kimel c/ Argentina, Fondo, Reparaciones y Costas", sentencia del 2 de mayo de 2008, Serie C N.º 177; Corte I.D.H., "Caso Tristán Donoso c/ Panamá, Excepción preliminar, Fondo, Reparaciones y Costas", sentencia del 27 de enero de 2009, Serie C N.º 193; Corte I.D.H., "Caso Ríos *et al.* c/ Venezuela, Excepciones preliminares, Fondo, Reparaciones y Costas", sentencia del 28 de enero de 2009, Serie C N.º 194; Corte I.D.H., "Caso Perozo y otros c/ Venezuela, Excepciones preliminares, Fondo, Reparaciones y Costas", sentencia del 28 de enero de 2009, Serie C N.º 195; Corte I.D.H., "Caso Usón Ramírez c/ Venezuela, Excepción preliminar, Fondo, Reparaciones y Costas", sentencia del 20 de noviembre de 2009, Serie C N.º 207; Corte I.D.H., "Caso Uzcátegui y otros c/ Venezuela, Fondo y Reparaciones", sentencia del 3 de septiembre de 2012, Serie C N.º 249; Corte I.D.H., "Caso Fontevecchia y D`Amico c/ Argentina, Fondo, Reparaciones y Costas", sentencia del 29 de noviembre de 2011, Serie C N.º 238.

sobre el Derecho a la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos[25] y la Declaración de Principios sobre Libertad de Expresión[26], ha extraído de las decisiones los siguientes estándares, entre otros:

1. Conforme al artículo 13 de la Convención Americana, la libertad de expresión es un derecho que corresponde a todas las personas, en igualdad de condiciones y sin discriminación de ningún tipo.
2. El artículo 13 de la Convención Americana establece el derecho de toda persona a la libertad de expresión, y estipula que este derecho comprende la "libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección". En su interpretación sobre el alcance del derecho de libertad de expresión, la Declaración de Principios sobre Libertad de Expresión, emitida por la Comisión Interamericana de Derechos Humanos, indica que este derecho fundamental e inalienable se refiere a la expresión humana "en todas sus formas y manifestaciones", y que alcanza al derecho de toda persona, en igualdad de condiciones, a "recibir, buscar e impartir información por cualquier medio de comunicación", así como el "derecho a comunicar sus opiniones por cualquier medio y forma". La Declaración de Principios también señala expresamente que toda persona tendrá derecho "a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados", y también a "actualizarla, rectificarla y/o enmendarla" si fuera necesario, además del derecho de "acceso a la información en poder del Estado".
3. En principio, todas las formas de discurso están protegidas por el derecho a la libertad de expresión, independientemente de su contenido y de la mayor o menor aceptación social y estatal con la que cuenten. Esta presunción general de cobertura de todo discurso expresivo se explica por la obligación primaria de neutralidad del Estado ante los contenidos y, como consecuencia, por la necesidad de garantizar que, en principio, no existan personas, grupos, ideas o medios de expresión excluidos *a priori* del debate público.

---

[25] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, *Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos*, OEA Ser.L/V/II, 30 de diciembre de 2009.

[26] Organización de los Estados Americanos, *Declaración de Principios sobre Libertad de Expresión,* 19 de octubre de 2000.

4. De particular importancia es la regla según la cual la libertad de expresión debe garantizarse no solo en cuanto a la difusión de ideas e informaciones recibidas favorablemente o consideradas inofensivas o indiferentes, sino también en cuanto a las que ofenden, chocan, inquietan, resultan ingratas o perturban al Estado o a cualquier sector de la población. Así lo exigen el pluralismo, la tolerancia y el espíritu de apertura, sin los cuales no existe una sociedad democrática. En este sentido, la Comisión ha señalado la particular importancia que tiene proteger a la libertad de expresión "en lo que se refiere a las opiniones minoritarias, incluyendo aquellas que ofenden, resultan chocantes o perturban a la mayoría"; y se ha enfatizado que las restricciones a la libertad de expresión "no deben 'perpetuar los prejuicios ni fomentar la intolerancia'".
5. La censura previa, interferencia o presión directa o indirecta sobre cualquier expresión, opinión o información difundida a través de cualquier medio de comunicación oral, escrito, artístico, visual o electrónico, debe estar prohibida por la ley. Las restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión.
6. Como ha sido interpretado en la jurisprudencia del sistema interamericano, el artículo 13.2 de la Convención exige que se reúnan las tres condiciones siguientes para que resulte admisible una limitación a la libertad de expresión: (1) la limitación debe haber sido definida en forma precisa y clara a través de una ley formal y material; (2) la limitación debe estar orientada al logro de objetivos imperiosos autorizados por la Convención Americana, y (3) la limitación debe ser necesaria en una sociedad democrática para el logro de los fines imperiosos que se buscan; estrictamente proporcionada a la finalidad perseguida; e idónea para lograr el objetivo imperioso que pretende lograr.

La Corte Interamericana de Derechos Humanos también ha emitido decisiones que prohíben la censura previa. En un caso de 2001 relativo a una violación del artículo 13 de la Convención Americana sobre Derechos Humanos, la Corte I.D.H. analizó los argumentos presentados en la Opinión Consultiva 5 (OC-5) sobre libertad de expresión. La Corte abordó en un primer momento las dos dimensiones de la libertad de expresión, e insistió en el "estándar

democrático". Lo novedoso de este pronunciamiento fue la interpretación del concepto de censura previa en la Convención. La Corte dispuso que el "artículo 13.4 de la Convención establece una excepción a la censura previa, ya que la permite en el caso de los espectáculos públicos pero únicamente con el fin de regular el acceso a ellos, para la protección moral de la infancia y la adolescencia. *En todos los demás casos, cualquier medida preventiva implica el menoscabo a la libertad de pensamiento y de expresión*"[27].

Ninguno de los casos en los cuales se invocó la DMCA para retirar de Internet contenidos de usuarios reúne estas condiciones, que posibilitarían que su censura sea admisible. Las características de estos casos, en cuanto a su contenido y las condiciones necesarias para imponer restricciones, los convierten en expresiones protegidas conforme a los estándares interamericanos.

3. Sistema europeo de derechos humanos

El derecho de libertad de expresión e información se encuentra garantizado en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

El artículo 10 dispone[28]:

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.
2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la

---

27 Bertoni, Eduardo, "*The Inter-American Court of Human Rights and the European Court of Human Rights: A dialogue on freedom of expression standards",* en: *European Human Rights Law Review,* Vol. 3, 2009, pp. 332-353. El resaltado es propio.

28 Consejo de Europa, *Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales*, reformado por los Protocolos N.º 11 y 14, 4 de noviembre de 1950, (ETS 5).

> prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

Si bien el Convenio describe circunstancias en las cuales el ejercicio de este derecho "podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática", también "reduce sustancialmente la posibilidad de intromisión en el derecho a expresar, recibir e impartir información e ideas. La intromisión por parte de autoridades públicas solamente será admisible cuando se cumplan una serie de condiciones rigurosas: que las restricciones o sanciones estén 'previstas por la ley', tengan un 'fin legítimo' y, por último y sobre todo, resulten 'necesarias, en una sociedad democrática'"[29]. El Tribunal Europeo de Derechos Humanos considera que la libertad de debate político, en particular, es "uno de los elementos más centrales del concepto de sociedad democrática". Dada la importancia de la libertad de expresión en una democracia, "se necesitarán motivos muy sólidos para justificar restricciones al discurso político"[30].

El profesor Dirk Voorhoof ha señalado en este sentido: "El reconocimiento por el Tribunal Europeo de un efecto horizontal del artículo 10 y de las obligaciones positivas que tienen los Estados Miembros de proteger el derecho de libertad de expresión ha ampliado incluso más el alcance de tal derecho en Europa"[31].

Si bien los tipos de expresiones en los casos analizados no quedan alcanzados por la competencia del Tribunal Europeo, sí cumplen los estándares expuestos en el Convenio Europeo.[32] Las cancelaciones efectuadas invocando la DMCA no reúnen las condiciones rigurosas que resultan necesarias para interferir en el derecho de libertad de expresión.

---

[29] Voorhoof, Dirk, "*The right to freedom of expression and information under the European Human Rights System: Towards a more transparent democratic society",* en: *EUI Working Papers*, 2014, disponible en: http://bit.ly/1QEQ9te.

[30] Leach, Phillip, *Taking a case to the European Court of Human Rights,* Nueva York, Oxford University Press, 2011.

[31] Voorhoof, Dirk, *supra* nota 29.

[32] Desde las primeras etapas (Opinión Consultiva OC-5) y hasta los casos más recientes dirimidos por la Corte Interamericana, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha tenido importantes repercusiones. *Véase,* Bertoni, Eduardo, *supra* nota 27.

VI. El futuro de la DMCA y la libertad de expresión: recomendaciones y alternativas a futuro

La mayoría de los activistas y académicos que trabajan en temas de Internet coinciden[33] en que, sin la disposición sobre cancelaciones de la DMCA, numerosos proveedores de servicios en línea no podrían alojar ni transmitir contenidos generados por usuarios debido al temor a incurrir en responsabilidad por violación de derechos de autor.[34] Sin embargo, también admiten que, tradicionalmente, la Ley ha sido usada de manera indebida para inhabilitar el acceso a contenidos que están inequívocamente protegidos por los estándares internacionales y regionales de libertad de expresión. Entonces, la cuestión es cómo conciliar una norma imperfecta, pero necesaria, como la DMCA con la transgresión de principios democráticos centrales que esta permite.

La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) señala que gran parte de las críticas a la DMCA se relacionan con el hecho de que esta se presta a abusos. Observa que la DMCA "facilita la autocensura al asignar al intermediario un rol cuasi judicial, responsable de evaluar la legalidad de contenidos"[35]. Por ende, abordar el uso indebido de la DMCA requiere considerar atentamente la responsabilidad de los intermediarios (es decir, la responsabilidad de proveedores de servicios de internet, motores de búsqueda, redes sociales y otros sitios que alojan información) por los contenidos de los usuarios. Ante una sucesión de cancelaciones basadas en reclamos por derechos de autor poco plausibles o inexistentes, es difícil no caer en la tentación de sostener que la responsabilidad corresponde a estos intermediarios en línea. Una posibilidad sería entonces insistir en que los proveedores de servicios analicen los reclamos más minuciosamente; es decir, al recibir cada solicitud de cancelación, los proveedores podrían evaluar

---

33 *Véase,* Samuel, Julie, "*DMCA copyright policies: Staying in the safe harbors while protecting your users",* en: *Electronic Frontier Foundation Deeplinks Blog,* 11 de febrero de 2011, disponible en: http://bit.ly/1QEQjAO.

34 La DMCA, en particular una sección de esta norma que lleva el título "Ley de Limitación de la Responsabilidad por Violaciones de Derechos de Autor en Línea" (*Online Copyright Infringement Liability Limitation Act*), contempla en su, sección 512, una excepción de "puerto seguro" para intermediarios que los ampara de responsabilidad por violación de derechos de autor en numerosas circunstancias. Para obtener información adicional sobre los denominados "puertos seguros" y la responsabilidad conforme a la DMCA, *véase,* Boyle, James y Jenkins, Jennifer, *Intellectual property: Law & the information society - cases and materials*, Duke Law School, 2014.

35 MacKinnon, Rebecca y otros, *Fostering freedom online: The role of Internet intermediaries,* Paris, UNESCO, 2014, disponible en: http://bit.ly/1JMyLx5.

la pretensión en términos de uso justo, y conceder o desestimar el pedido en función de esto. Sin embargo, evaluar reclamos por violación de derechos de autor en cada caso en particular sería una tarea colosal, y sin duda afectaría la capacidad de los proveedores de alojar y transmitir una diversidad de contenidos al ritmo que lo hacen actualmente.

Electronic Frontier Foundation (EFF), una organización sin fines de lucro dedicada a derechos digitales, apoya la formulación de una "política justa sobre infracción reincidente"[36]. Este enfoque, que considera múltiples aspectos, está más centrado en el usuario que el proceso actual. Sugiere notificar oportunamente a los usuarios cuando se hayan planteado reclamos contra ellos y otorgarles oportunidades efectivas de contestar estas notificaciones e incluso contactar a los titulares del derecho de autor. EFF adhiere a los señalamientos de otros actores que han identificado fallas en el sistema actual de notificación y cancelación, y recomienda poner fin a la práctica de eliminación instantánea y, en vez de ello, favorecer una comunicación abierta con los usuarios sobre contenidos violatorios, para que puedan responder a pedidos de cancelación y evitar la suspensión automática de sus cuentas.[37] EFF sostiene, asimismo, que debería existir una especie de política de "confianza" que establezca garantías adicionales -como una mayor cantidad de "infracciones" o un proceso de apelación por vía rápida- para usuarios que no tengan antecedentes considerables de publicación de materiales violatorios. Estas medidas, asevera EFF, podrían empoderar a usuarios a oponerse a cancelaciones abusivas, sin que esto suponga una carga indebida para intermediarios en línea.

Por otra parte, Global Network on Copyright Users' Rights recomienda un enfoque más flexible de la política sobre derechos de autor. Propusieron una Excepción Modelo Flexible a los Derechos de Autor, que podría adaptarse a la mayoría de las leyes sobre la materia, y que propone excepciones y pautas adicionales para la interpretación e implementación de derechos de autor. En su disposición más importante señala:

---

36 *Véase,* Samuel, Julie*, supra* nota 33.

37 Por ejemplo, la profesora Dawn Nunziato señala que el sistema de notificación y cancelación de la DMCA brinda un margen considerable a los titulares de derechos de autor para vigilar el uso de sus contenidos. Asevera que la disposición existente "permite que el titular de un derecho de autor obtenga el equivalente a una medida inhibitoria temporal -una orden judicial que dispone quitar el contenido presuntamente violatorio-, pero sin el beneficio de un proceso judicial". Nunziato, Dawn, "*Keeping the Internet free in the Americas",* CELE – Universidad de Palermo, 2011, disponible en: http://bit.ly/1PPjJcj.

> Además de los usos expresamente autorizados por la ley, cualquier uso que promueva objetivos económicos, sociales y culturales generales no será violatorio cuando su naturaleza y alcance sean apropiados a sus fines y no menoscaben indebidamente los intereses legítimos del titular de derechos de autor, tomando en cuenta los intereses legítimos de creadores, usuarios, terceros y el público.[38]

Por lo tanto, se enfoca en la DMCA y procura ampliar sus parámetros en vez de solamente modificar su aplicación. La excepción modelo refleja el reconocimiento de la necesidad de repensar las implicancias de la protección de los derechos de autor en la era digital y tomar en cuenta el interés público y de los usuarios.

En 2013, ARTICLE 19, una organización sin fines de lucro dedicada a la libertad de expresión, se sumó a otros grupos para formular los "Principios del derecho a compartir", que procuran alcanzar un equilibrio entre el derecho de libertad de expresión y la integridad de los derechos de autor. Algunas de las principales recomendaciones incluyen despenalizar las violaciones de derechos de autor que no sean de tipo comercial; no bloquear páginas web sin una orden judicial; medidas para promover el acceso al conocimiento y la cultura; y la evaluación de aspectos de transparencia y derechos humanos en tratados comerciales que contengan disposiciones sobre protección de derechos de autor.[39] Sus recomendaciones ofrecen mejores prácticas para abordar cuestiones transnacionales de derechos de autor, reconociendo prioridad al derecho de libertad de expresión y el acceso a bienes culturales[40]

Algunos grupos han propuesto medidas más extremas para disuadir cancelaciones abusivas conforme a la DMCA. Una experta en derecho sugiere enfocar la atención en un actor completamente distinto: la persona que plantea el reclamo por violación de derechos de autor. Sostiene que el Congreso prevé un mecanismo para disuadir cancelaciones indebidas, a través del reclamo por falsedad (*misrepresentation claim*), que puede hacerse valer cuando se asevere falsamente que un contenido es violatorio. Si los usuarios que han sufrido cancelaciones injustamente plantearan estas acciones con mayor frecuencia, podrían contrarrestar el uso indebido de la DMCA para censurar expresiones

---

38 American University Washington College of Law, "*Model Flexible Copyright Exception*", 2012, disponible en: http://bit.ly/1KnHETU.

39 *Véase,* Guillemin, Gabrielle, "*Copyright week: Why the right to share principles matter in the digital age",* en: *Article 19*, 17 de enero de 2014, disponible en: http://bit.ly/1dIGyRw.

40 *Véase,* Article 19, *The right to share: Principles on freedom of expression and copyright in the digital age*, 2013, disponible en: http://bit.ly/1NODEqj.

en línea, disuadiendo a los titulares de derechos de autor o a sus representantes de plantear pretensiones improcedentes.[41]

VII. Conclusiones

Si bien cada una de estas recomendaciones propone pasos importantes para reducir al mínimo las pretensiones abusivas sobre violación de derechos de autor, ninguna consigue equilibrar completamente la carga que sobrellevan los proveedores de servicios de internet y los usuarios. Cualquier escenario en el cual la DMCA sea el árbitro último con respecto a los contenidos digitales importa una responsabilidad compartida entre ciudadanos y empresas. No es razonable que los intermediarios en línea deban examinar cada pedido individual de cancelación, del mismo modo en que tampoco sería razonable que personas comunes tuvieran que defender una y otra vez su derecho a generar y subir contenidos que no son violatorios.

Tal vez un tercero independiente, como un grupo asesor internacional, podría contribuir a que se llegue a consensos en esta área tan compleja, aportando pautas neutrales a compañías de internet sobre procedimientos de protección de derechos de autor. Esto ayudaría a alivianar algunas de las cargas que pesan sobre los proveedores y, al mismo tiempo, demostraría la voluntad del sector de tecnología de formar parte de la solución a las violaciones del derecho de libertad de expresión en línea. No obstante, encontrar el equilibrio justo entre proveedores de servicios y usuarios requiere la voluntad de ambas partes de invertir en la defensa del derecho de libertad de expresión. Los proveedores de servicios en línea como Google, YouTube, Facebook, Twitter y otros distribuidores deberían reconsiderar sus protocolos actuales teniendo esto presente, y solicitar comentarios a usuarios y actualizar sus políticas para asegurar que la DMCA siga contribuyendo a la innovación, sin silenciar expresiones.

41 *Véase,* Pallas Loren, Lydia, "*Deterring abuse of the copyright takedown regime by taking misrepresentation claims seriously",* en: *The Wake Forest Law Review*, 2011, disponible en: http://bit.ly/1o2FU8G.

Responsabilidad de intermediarios y derecho al olvido

Aportes para la discusión legislativa en Argentina

Verónica Ferrari y Daniela Schnidrig[1]

Resumen

Hoy en día en Argentina existen diversos proyectos de ley que buscan abordar una cuestión clave a la hora de pensar en la regulación de internet: ¿qué responsabilidad le cabe a los intermediarios? Este artículo busca, en primer lugar, definir qué son los intermediarios en internet y analizar qué tipos de responsabilidad les pueden caber por la información que aparece en línea. En este sentido, se buscará explicar qué es el llamado derecho al olvido –fundamentalmente, en los términos establecidos en el fallo "Google Spain"[2]– y cómo se relaciona con la responsabilidad de los intermediarios.

A lo largo del documento se intentará explicar por qué trasladar esos mismos criterios a nuestra legislación sobre responsabilidad de intermediarios puede presentar riesgos para la libertad de expresión y el acceso a la información. Finalmente, haremos una serie de aportes y recomendaciones sobre cómo se deberían abordar estos temas en la legislación local a fin de garantizar el respeto a la libertad de expresión y al acceso a la información en internet.

---

1 Este documento fue elaborado por Verónica Ferrari y Daniela Schnidrig, investigadoras del Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. Actualmente, Daniela Schnidrig se desempeña como Project Manager en Global Partners Digital.

2 TJUE, "Google Spain, S.L., Google Inc. c/ Agencia Española de Protección de Datos, Mario Costeja González", sentencia del 13 de mayo de 2014, disponible en: http://bit.ly/1JzKzqV.

I. Responsabilidad de intermediarios

1. Intermediarios en internet. ¿Qué son y cuál es su rol?

Los intermediarios son actores que hacen posible muchas de las actividades de nuestra vida cotidiana y, a la vez, definen la manera en las que las desarrollamos.[3] Según las teorías que abordan el tema de los intermediarios en general,[4] estos actúan como "guardianes" en tanto controlan y previenen ciertos comportamientos "indeseables". Los intermediarios, entonces, aparecen como una alternativa a los Estados en materia regulatoria: el control se desplaza a estos espacios privados.

Siguiendo la definición de la UNESCO,[5] publicada en una investigación sobre la base de estudios de caso en diferentes países, entendemos por intermediarios en internet a los "servicios que median las comunicaciones en línea y que permiten diversas formas de expresión en línea".[6] Por otro lado, el documento que sirvió de base para la elaboración de los Principios de Manila sobre responsabilidad de intermediarios los define como aquellos que "llevan a cabo o facilitan transacciones entre terceros en internet", ya sea porque dan acceso, alojan, transmiten o indexan contenidos, productos y servicios generados por terceros[7]; por ejemplo, los proveedores de servicios de conexión, los buscadores, las redes sociales, entre otros.

Argentina, al igual que gran parte de América Latina, se encuentra en un momento clave del debate sobre la regulación de internet, en general, y de qué forma deben ser regulados intermediarios, en particular. A continuación abordaremos los distintos tipos de responsabilidad que se les pueden aplicar y los inconvenientes que puede acarrear la falta de regulación adecuada y específica en la materia.

---

3 Cortés Castillo, Carlos, "Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital", en: Bertoni, Eduardo (comp.), *Internet y Derechos Humanos. Aportes para la discusión en América Latina*, Buenos Aires, CELE - Universidad de Palermo, 2014, p. 64, disponible en: http://bit.ly/NVQ5K5.

4 *Véase*, Kraakman, Reinier H., *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy,* en: *Journal of Law, Economics, & Organization*, Vol. 2, No. 1, Oxford University Press, 1986; y, Laidlaw, Emily, *A framework for identifying Internet information gatekeepers,* en: *International Review of Law, Computers & Technology,* Vol. 24, No. 3, 2010, citados en el artículo de Cortés Castillo.

5 MacKinnon, Rebecca y otros, *Fostering Freedom Online. The Role of Internet Intermediaries*, París, UNESCO, 2014, disponible en: http://bit.ly/1JMyLx5.

6 *Ibíd.*, p. 9. Traducción propia.

7 *Ibíd.*, p. 19. Traducción propia.

2. Breve introducción a la regulación de intermediarios

¿Qué significa "responsabilidad de intermediarios? ¿En qué casos podría discutirse la responsabilidad del intermediario? En esta sección analizaremos los distintos modelos de responsabilidad que se pueden aplicar a estos actores.

Puede ocurrir que usuarios publiquen, compartan o diseminen contenidos que violen derechos de terceros. Por ejemplo, fotos de una persona sin su consentimiento. Tomemos el caso de una persona que publica fotos de otra persona sin su consentimiento. Esto representa una violación a la privacidad de quien aparece en las fotos. ¿Qué podría hacer la persona damnificada? Sin dudas, podría reclamar al usuario que publicó la foto. Por ejemplo, podría exigir que elimine la imagen e incluso podría demandar una compensación monetaria en concepto de los daños sufridos.

La persona que publicó la foto lo hizo a través de distintos intermediarios: el proveedor de servicios de internet, aquel que da alojamiento al sitio web y, probablemente, un buscador que haya indexado la publicación en su motor de búsqueda. ¿Podría la persona damnificada reclamar algo a estos intermediarios? Esta es la cuestión en debate cuando hablamos de la responsabilidad de los intermediarios.

Podemos distinguir cuatro modelos de responsabilidad de intermediarios: la inmunidad absoluta, la responsabilidad objetiva, la responsabilidad subjetiva, y la responsabilidad condicionada.[8] A continuación, describiremos brevemente cada modelo, explicando sus características, y evaluando sus consecuencias positivas y negativas.

a. Inmunidad absoluta. Bajo este régimen, ningún intermediario sería responsable por ningún tipo de contenido ilegal publicado o compartido por las personas a través de su servicio. El beneficio de este tipo de responsabilidad es el respeto por el derecho a la libertad de expresión: los intermediarios no temerán por su posible responsabilidad respecto a los contenidos de terceros, por lo tanto, no tendrán incentivos para monitorear, bloquear ni filtrar contenidos.

Sin embargo, este enfoque ha recibido críticas. Algunos autores han señalado que la inmunidad absoluta causaría un desequilibrio con otros derechos,

---

[8] *Véase también*, Meléndez Juarbe, Hiram, "Intermediarios y libertad de expresión", en: Bertoni, Eduardo (comp.), *Hacia una Internet libre de censura. Propuestas para América Latina,* Buenos Aires, CELE - Universidad de Palermo, 2012, pp. 116-117, disponible en: http://bit.ly/1QFZMpg. *Véase,* Cortés Castillo, Carlos, *supra* nota 3, pp. 74-83.

como la privacidad o la honra, ya que los intermediarios no tendrán ningún tipo de aliciente para filtrar contenidos violatorios de estos derechos.[9]

b. Responsabilidad objetiva. Bajo este régimen, el intermediario siempre sería responsable por los contenidos que los usuarios expresen a través de ellos, sin importar si tuvo conocimiento de dichos contenidos. La única forma para el intermediario de librarse de responsabilidad sería monitorear contenidos constantemente y filtrar o bloquear aquellos que considere que podrían llegar a ser ilícitos y que podrían comprometer su responsabilidad.[10]

Este es el enfoque más restrictivo y es duramente criticado porque puede violar la libertad de expresión. Un régimen de responsabilidad objetiva pone en manos del intermediario la decisión sobre la legalidad de los contenidos. Si el intermediario es responsabilizado por los contenidos de terceros tenderá a filtrar y bloquear cualquier contenido que considere que, eventualmente, podría hacerlo responsable.

c. Inmunidad condicionada. Bajo este régimen, el intermediario no será responsable, siempre y cuando cumpla con ciertas condiciones o requisitos. Se le ofrece al intermediario un "puerto seguro", es decir, mientras cumpla con ciertos deberes concretos no será responsable por contenidos ilegales de terceros.[11]

Hay distintas variantes del régimen de inmunidad condicionada. El modelo *notice and take down* –notificación y retiro– ofrece, al usuario que considera que un contenido es ilegal, la posibilidad de notificar al intermediario para que este, luego, filtre dicho contenido. Como explicaremos más adelante, este modelo es el que se aplica en el fallo de la justicia europea sobre el derecho al olvido.

En cambio, en el modelo *notice and notice* –notificación y notificación–, el usuario notifica al intermediario de la existencia de contenido ilegal y este, a su vez, deberá notificarlo a quien generó el contenido.

Este tipo de modelo de responsabilidad puede provocar la remoción excesiva de contenidos, afectando la libertad de expresión.

d. Responsabilidad subjetiva. Bajo este régimen, debe analizarse la conducta del intermediario para definir si ha tomado todas las precauciones necesarias o ha sido negligente.

---

9 *Véase*, Cortés, Carlos, *supra* nota 3, p. 77.
10 *Véase,* MacKinnon, Rebecca, y otros, *supra* nota 5.
11 *Véase,* Cortés Castillo, Carlos, *supra* nota 3, p 14.

3. El marco legal argentino sobre responsabilidad de los intermediarios. Análisis de la jurisprudencia local y sus inconsistencias

Argentina no tiene normativa específica sobre responsabilidad de intermediarios, lo cual representa un problema para la jurisprudencia. El nuevo Código Civil y Comercial de la Nación establece dos regímenes de responsabilidad civil: responsabilidad subjetiva y responsabilidad objetiva. Como no hay un régimen legal específico para aplicar en casos sobre responsabilidad de intermediarios, el Poder Judicial debe recurrir a estos principios generales de la responsabilidad civil a la hora de pronunciarse en estos casos.

Un caso es el del empresario Esteban Bluvol,[12] que demandó a Google cuando se enteró de la existencia de un *blog* con su nombre, creado por otra persona, que publicaba contenido agraviante y que lo perjudicaba profesionalmente. Con respecto a esta demanda, dos tribunales que intervinieron en el caso aplicaron regímenes de responsabilidad distintos.

El juez de primera instancia hizo lugar a la demanda y condenó a los buscadores a otorgar una indemnización sobre la base de la responsabilidad objetiva. Luego, el tribunal de segunda instancia revirtió la decisión y desestimó la aplicación de responsabilidad objetiva. La Cámara consideró que Google, en tanto intermediario, no debe responder de forma automática por conductas ilícitas de terceros y que, dada la inmensa cantidad de información que circula por internet, es imposible realizar un control previo de todo lo que se difunde.[13] Si bien el tribunal consideró que Google era responsable, lo hizo bajo un régimen subjetivo de responsabilidad. Es decir, analizó cuál fue la conducta del buscador que, según el tribunal, en este caso había sido negligente.

Otros casos emblemáticos son los de celebridades y artistas que demandan a buscadores. Por ejemplo, el caso Da Cunha*,* en el que una cantante demandó a los buscadores Google y Yahoo!. Da Cunha solicitaba el cese del uso de su imagen en sitios pornográficos, así como una indemnización por daños y perjuicios. La Cámara de Apelaciones se pronunció en el caso, aplicando un régimen subjetivo de responsabilidad, y señaló que el buscador podrá considerarse responsable cuando es notificado y no remueve el contenido.[14] Da Cunha apeló esta decisión y la Corte Suprema rechazó el recurso. Más

---

12 *Véase,* Cámara Nacional de Apelaciones en lo Civil, Bluvol, Esteban Carlos c / Google Inc. y otros s/ daños y perjuicios", 5 de diciembre de 2012, disponible en: http://bit.ly/1KnIb8e.

13 *Ibíd*., p 4.

14 *Véase,* Cámara Nacional de Apelaciones en lo Civil, "D. C. V. c/ Yahoo de Argentina SRL y otro s/ Daños y Perjuicios", 10 de agosto de 2010.

adelante analizaremos en detalle las decisiones del máximo tribunal en este tipo de casos.

Otro de los ejemplos que muestra a las claras la problemática de la falta de regulación específica sobre responsabilidad de los intermediarios así como el desconocimiento de los tribunales en el tema, es el caso de una medida cautelar otorgada por un tribunal de primera instancia que ordenó a Google bloquear de sus resultados de búsqueda todos aquellos sitios que contuvieran el video de la actriz Florencia Peña manteniendo relaciones sexuales.[15] Este tipo de medidas son muy problemáticas para la libertad de expresión ya que no apuntan a bloquear una URL definida, sino que ordenan el bloqueo de todas aquellas URL que tengan conectores alusivos al video. Esto puede resultar en la eliminación de contenido lícito, afectando así la libertad de expresión.

El fallo Carrozo, de diciembre de 2013, es otro ejemplo de una sentencia judicial contraria a la libertad de expresión. En este fallo la Cámara de Apelaciones ordenó que Google y Yahoo! compensaran a la modelo por el uso de su imagen en sitios pornográficos. En su sentencia, el tribunal aplicó un régimen objetivo de responsabilidad porque consideró que los buscadores llevan a cabo una actividad riesgosa, lo cual los hace automáticamente responsables por los daños que puedan ocurrir.[16]

4. Análisis de la jurisprudencia de la Corte Suprema de Justicia sobre responsabilidad de intermediarios

Analizaremos el caso Rodríguez[17] de la Corte Suprema de Justicia de la Nación y los estándares dispuestos por el máximo tribual. El de Belén Rodríguez es uno de los tantos casos en que distintas celebridades, que encuentran imágenes suyas en sitios pornográficos o de oferta sexual, se ven lesionadas en su honor e inician acciones legales contra los motores de búsqueda.

¿Qué es lo que solicitan en estos casos? En líneas generales, podemos distinguir entre dos peticiones comunes. En primer lugar, solicitan la eliminación de los contenidos que, alegan, violan sus derechos. En segundo lugar, la solicitud de una indemnización por los daños sufridos.

---

15 V*éase,* Juzgado Nacional de Primera Instancia en lo Civil N° 72, “Peña María Florencia c/ Google s/ ART. 250 C.P.C”, Incidente Civil -Expte. N° 35.613/2013.

16 Cámara Nacional de Apelaciones en lo Civil, “Carrozo, Evangelina c/ Yahoo de Argentina SRL y otro s/ daños y perjuicios”, 10 de diciembre de 2013, disponible en: http://bit.ly/1QERfoP.

17 *Véase,* CSJN, "Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios", 28 de octubre de 2014, disponible en: http://bit.ly/1b4lxAI.

En el caso Rodríguez, la actora demandó a los buscadores Google y Yahoo! solicitando, por un lado, la eliminación de todos aquellos sitios web que la relacionaran con servicios de oferta sexual y, por otro lado, una indemnización por las lesiones a su honor y por el uso indebido de su imagen.

La Cámara de Apelaciones decidió analizar la conducta de los buscadores –aplicando así un régimen subjetivo–, y concluyó que no hubo negligencia porque la damnificada nunca los intimó directamente para que removieran los contenidos sino que inició acciones judiciales directamente. Sin embargo, la Cámara sostuvo que el uso de *thumbnails*[18] por parte de Google sí consistía en un uso no autorizado de la imagen de Rodríguez.

El caso, finalmente, llegó a la Corte Suprema de Justicia que –tras recibir *amicus curiae* y realizar audiencias públicas para escuchar la opinión de expertos en la materia[19]– se pronunció el 28 de octubre de 2014. En su fallo cita instrumentos de organismos internacionales de derechos humanos, como el informe del Relator Especial de la ONU para la Libertad de Opinión y de Expresión[20] y la Declaración Conjunta de las Relatorías por la Libertad de Expresión de 2011[21], y destaca que la libertad de expresión debe aplicarse también en internet.[22]

A continuación, analizaremos la posición de la Corte sobre distintas cuestiones:

- Respecto del pedido de la actora de aplicar responsabilidad objetiva: la Corte sostiene en su decisión que las leyes deben interpretarse de forma en que concuerden mejor con los derechos constitucionales. Ante la inexistencia legal de una obligación de los buscadores de supervisar y monitorear contenidos, lógicamente, no debería haber responsabilidad si no lo hacen. Además de ser injusto, esto daría a los intermediarios incentivos contrarios a la libertad de expresión, señala el máximo

---

18 Las imágenes pequeñas que se usan como vista previa de una página web.

19 Es posible ver los videos de las audiencias en el sitio del Centro de Información Judicial, disponibles en: http://bit.ly/1Eznl2I y en: http://bit.ly/20mHeEB.

20 *Véase,* ONU, Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión, A/66/290, 2011, disponible en: http://bit.ly/20Eiuo4.

21 *Véase,* ONU, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión y otros, *Declaración Conjunta sobre Libertad de Expresión e Internet*, 2011.

22 El fallo de la Corte no fue unánime. Los jueces Lorenzetti y Maqueda emitieron un voto en disidencia respecto de la posibilidad de garantizar acciones de tutela preventiva a fines de evitar que se produzca este tipo de casos, y respecto de la cuestión de los *thumbnails*.

tribunal. En definitiva, concluye la Corte, aplicar un régimen de responsabilidad objetiva sería contrario a la libertad de expresión.[23]

- ¿Cuándo se responsabilizará al buscador? En los casos en que, teniendo efectivo conocimiento de la ilicitud de un contenido, no actúe diligentemente.[24]
- ¿Qué se entiende por "efectivo conocimiento"? La Corte responde a esta inquietud en forma de *obiter* –esto es, lo analiza como algo suplementario ya que no es necesario para decidir el caso en particular–, y se pregunta si es necesaria la notificación de una autoridad competente o basta con la notificación privada.

  En principio, aclara la Corte en su decisión, será necesaria la "notificación judicial o administrativa competente, no bastando la simple comunicación del particular que se considere perjudicado y menos la de cualquier persona interesada"[25].

  Sin embargo, señala la Corte, podría haber casos en los que, excepcionalmente, bastaría con una comunicación fehaciente del damnificado o de un tercero. El máximo tribunal se refiere a estos casos excepcionales como de "manifiesta ilicitud", en los que la naturaleza ilícita es "palmaria y resulta directamente de consultar la página señalada"[26]. En estos casos excepcionales, sería necesario actuar de forma urgente, y esperar a una resolución judicial podría lesionar derechos.
- ¿Qué casos serían de "manifiesta ilicitud"? La Corte no establece una definición clara sino que da algunos ejemplos como pornografía infantil, datos que faciliten la comisión de delitos, que pongan en peligro la vida o la integridad física de alguna o muchas personas, entre otros.

  Este estándar, entendemos, resulta un poco confuso ya que la definición de algunos de estos casos puede ser demasiado amplia. Entendemos que hay cuestiones que requieren atención y una reacción urgente como, por ejemplo, la protección de menores. Para estos casos excepcionales, sin embargo, entendemos que debería preverse un procedimiento judicial especial que contemple su gravedad y otorgue una respuesta expedita. De lo contrario, se estaría delegando en el buscador la decisión de qué es "manifiestamente ilícito" y qué no.
- ¿Qué criterio debe adoptarse respecto de los *thumbnails*? La Corte

---

23 *Véase,* CSJN, *supra* nota 17, considerando 16.
24 *Véase,* CSJN, *supra* nota 17, considerando 17.
25 *Véase,* CSJN, *supra* nota 17, considerando 18.
26 *Ibíd.*

entiende que el *thumbnail*, respecto de la imagen original "subida" a una página de Internet, tiene una función de mero "enlace". Es decir, los *thumbnails* dan una idea al usuario del contenido de la página para decidir si quiere o no acceder. La Corte, en su decisión, aclara que "la imagen original y el texto original –'subidos' a la página web– son responsabilidad exclusiva del titular de aquella, único creador del contenido"[27]. En conclusión, no se cuestiona que al creador del contenido pueda responsabilizárselo por dicha imagen, pero el buscador es un mero intermediario, no es creador de ese contenido, por lo tanto no debe atribuírsele responsabilidad.[28]

- Respecto del pedido de remoción de contenidos a través de una cautelar, la Corte enfatiza la prohibición de censura previa que establece el artículo 13 de la Convención Americana de Derechos Humanos, y sostiene que toda restricción o limitación a la libre expresión debe ser de interpretación restrictiva ya que toda censura tiene una fuerte presunción de inconstitucionalidad. Este principio solo podría ceder ante cuestiones absolutamente excepcionales que, en el caso, no están dadas.

Unos meses más tarde, en diciembre, la Corte Suprema reforzó este precedente al resolver dos casos similares.[29] En ambas sentencias, la Corte se remitió a lo resuelto en el fallo Rodríguez y rechazó las peticiones de las actoras.

- ¿Esto significa que los intermediarios nunca podrán ser responsables? No. Esta es una confusión común, pero debemos hacer una distinción. El principio establecido por la Corte es que los intermediarios no pueden ser responsables por el contenido generado por terceros. Sí podrán ser responsabilizados por su propia conducta.

Por ejemplo, si un intermediario recibe una orden judicial que ordene remover contenidos y no lo hace, podrá ser responsabilizado. Pero no será en virtud de los contenidos ilegales sino en virtud de no acatar la orden judicial. En estos casos en particular, la Corte consideró que la conducta de los buscadores fue adecuada y, por lo tanto, no los responsabilizó.

---

27 *Véase,* CSJN, *supra* nota 17, considerando 20.
28 *Véase,* CSJN, *supra* nota 17, considerando 21.
29 *Véase,* CSJN, "Da Cunha, Virginia c/ Yahoo de Argentina S.R.L., y otro s/ daños y perjuicios", 30 de diciembre de 2014, disponible en: http://bit.ly/1GfxxIs. *Véase también,* CSJN, "Lorenzo, Bárbara c/ Google Inc., s/ daños y perjuicios", 30 de diciembre de 2014, disponible en: http://bit.ly/1JCeZVQ.

5. Recomendaciones de algunos organismos intergubernamentales y de organizaciones de la sociedad civil

Varios organismos intergubernamentales de derechos humanos sostienen que la regla debe ser la irresponsabilidad del intermediario por contenidos generados por terceros. Las relatorías de libertad de expresión sostuvieron lo siguiente en su Declaración Conjunta de 2011:

> (…) ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, *siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo* ('principio de mera transmisión').[30]

Las relatorías se pronuncian, de esta forma, en contra de un régimen objetivo de responsabilidad en tanto señalan que "imponer la responsabilidad objetiva en esta materia equivaldría a desincentivar radicalmente la existencia de los intermediarios necesarios para que Internet conserve sus características en materia de circulación de información"[31].

En definitiva, resume la Relatoría por la Libertad de Expresión de la OEA en su informe "Libertad de Expresión e Internet", los intermediarios no tienen –ni tienen que tener– la capacidad técnica para revisar contenidos ni tienen –o deben tener– el conocimiento jurídico necesario para identificar en qué casos un determinado contenido podría llegar a producir un daño dado que:

> (…) incluso si contaran con el número de operadores y abogados que les permitiera realizar este ejercicio, los intermediarios, en tanto actores privados, no necesariamente van a considerar el valor de la libertad de expresión al tomar decisiones sobre contenidos producidos por terceros que pueden comprometer su responsabilidad.[32]

---

30 ONU, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión y otros, *supra* nota 20,punto 2 (a). El destacado es de las autoras.

31 *Ibíd.*, párrafo 97.

32 Meléndez Juarbe, Hiram, *supra* nota 8, p. 111. Sobre los roles e incentivos hacia los intermediarios, *véase también,* Cortés Castillo, Carlos, *supra* nota 3; Naciones Unidas, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra* nota 20, párrafo 42. Disponible en: http://bit.ly/1PdxX7h; y, CIDH, Relatoría Especial para la Libertad de Expresión, Informe "Libertad de Expresión e Internet", 2013, párrafo 99.

A su vez, otros organismos han elaborado recomendaciones sobre el tema, como UNESCO en el informe sobre el rol de los intermediarios y la libertad en internet antes mencionado[33]. Entre otras cosas, dicho informe señala que la adopción de leyes y la regulación sobre intermediarios deben ser consistentes con las normas internacionales de derechos humanos y que las normas y políticas regulatorias sobre intermediarios deben desarrollarse consultando a todas las partes potencialmente afectadas –*stakeholders*–. Además, el informe enfatiza la importancia de la transparencia de los principios, normas y condiciones que regulan a los intermediarios (por ejemplo, publicar informes de transparencia), y pone énfasis en la importancia de proteger la privacidad de los usuarios para asegurar el pleno ejercicio de la libertad de expresión.[34]

Como mencionamos antes, en marzo de 2015 un grupo de organizaciones de la sociedad civil presentó y adoptó los Principios de Manila sobre responsabilidad de intermediarios.[35] La iniciativa buscó delinear una serie de principios que sirvan para la elaboración de leyes, regulaciones y políticas en materia de responsabilidad de los intermediarios sobre contenido publicado por terceros. Estos principios establecen que:

- Los intermediarios deben ser protegidos por ley de responsabilidad por el contenido de terceros.
- No debe requerirse la restricción de contenidos sin una orden emitida por una autoridad judicial.
- Las solicitudes de restricción de contenido deben ser claras, inequívocas, y respetar el debido proceso.
- Las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los *tests* de necesidad y proporcionalidad.
- Las leyes, órdenes y prácticas de restricción de contenido deben respetar el debido proceso.
- La transparencia y la rendición de cuentas deben ser incluidas dentro de la normativa, políticas y prácticas sobre restricción de contenido.[36]

---

33 MacKinnon, Rebecca, y otros, *supra* nota 5.

34 Se puede acceder a todas las recomendaciones en: *Ibíd*., pp. 12 y 13.

35 *Véase,* EFF y otros, "Principios de Manila para la responsabilidad de intermediarios", disponible en: http://bit.ly/1B1QhPl.

36 *Ibíd.* Traducción propia.

II. Derecho al olvido

1. Derecho al olvido: definiciones

Si bien el concepto de “derecho al olvido” no es nuevo,[37] en los últimos años el debate a su alrededor ha ido ganando protagonismo, especialmente en Europa. Esto es resultado, en gran medida, de una decisión del Tribunal de Justicia de la Unión Europea (TJUE)[38] de mayo de 2014. En esta decisión, el TJUE –basado en el marco regulatorio en materia de datos personales de la Unión Europea–, decidió que Google, y los motores de búsqueda en general, son responsables por el tratamiento de los datos personales que aparecen en los sitios web.[39]

Es decir, de acuerdo con el fallo, una persona puede pedir que determinada información personal que es inadecuada, no pertinente, desactualizada o excesiva en relación con los fines para los que se recolectó sea removida de los resultados de las búsquedas,[40] siempre que no exista interés público.[41] Y el gestor de un motor de búsqueda, siguiendo con el fallo, está obligado a eliminarla.[42] Retomando la clasificación que hicimos antes, el modelo de responsabilidad de intermediarios que se estaría aplicando en este fallo del TJUE es el de inmunidad condicionada, bajo el mecanismo de notificación y retiro –*notice and take down*–.

En realidad, más que del denominado derecho al olvido, esta decisión del tribunal europeo se trata de un “derecho a no ser indexado por el buscador”[43], dado que la información que el usuario o la usuaria pretende “olvidar”

---

37 Carlos Cortés Castillo, siguiendo a Paul Bernal, señala que el origen del derecho al olvido hay que rastrearlo en el concepto del derecho francés *droit à l'oubli* y del italiano *diritto all'oblio*, que en términos generales, “se entienden como ‘el derecho a silenciar eventos pasados de la vida que ya no están sucediendo’”, como crímenes que han ocurrido en el pasado y han prescrito. *Véase,* Cortés Castillo, Carlos, “Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital”, en: Bertoni, Eduardo (comp.), *Internet y Derechos Humanos. Aportes para la discusión en América Latina*, Buenos Aires, CELE, Universidad de Palermo, 2014, p. 135, disponible en: http://bit.ly/NVQ5K5. *Véase también,* Bernal, P. A., “*A Right to Delete?”*, en: *European Journal of Law and Technology*, Vol. 2, No.2, 2011, p. 1.

38 *TJUE*, “Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario *Costeja* González”, sentencia del 13 de mayo de 2014, disponible en: http://bit.ly/1JzKzqV.

39 *Ibíd.*, párrafos 83 y 85.

40 *Ibíd.,* párrafo 94.

41 *Ibíd.,* párrafo 81.

42 *Ibíd.,* párrafo 88.

43 Bertoni, Eduardo, “*The Right to Be Forgotten: An Insult to Latin American History*”, en: *The Huffington Post,* 24 de septiembre de 2014, disponible en: huff.to/1XnOoU1 La versión en

no se borra, permanece en el sitio donde está alojada. El buscador no puede olvidarla ni borrarla; lo que ocurre es que la información será más difícil de acceder ya que se obliga al buscador a que no nos dirija a ese sitio.[44]

2. El derecho al olvido, según el fallo europeo: una mala solución

El debate que reseñamos brevemente en el apartado anterior se da en un marco de transformaciones tecnológicas que afectan a la privacidad y al control de nuestra información en línea. Como señala el informe elaborado por Frank La Rue, ex relator especial de la ONU para la Promoción y Protección del Derecho a la Libertad de Expresión y Opinión, la expansión del uso de internet ha generado que preocupaciones válidas en torno a quién tiene acceso a determinada información personal, cómo se utiliza esa información y si se almacena, y por cuánto tiempo, se profundicen.[45]

Sin embargo, parafraseando al profesor Jonathan Zittrain, especialista en la materia de la Universidad de Harvard y uno de los fundadores del Berkman Center for Internet & Society, este "no tan nuevo derecho" constituye una solución pobre para un problema tan importante.[46]

Si bien el llamado fallo "Google Spain" no sienta jurisprudencia fuera de Europa, es problemático trasladar lineamientos similares a proyectos de ley en Argentina. A continuación, algunos de los problemas que traería trasladar esta "solución" a la europea:

- **Conflicto con derechos fundamentales como el acceso a la información y la libertad de expresión.** La decisión del tribunal europeo habla de la necesidad de buscar "un justo equilibrio" entre el derecho a la protección de datos personales y "el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión".[47] De todas formas, más adelante en ese mismo párrafo, señala que: "ciertamente, los derechos de esa persona [la que ve vulnerado

---

español, "El derecho al olvido: un insulto a la historia latinoamericana", puede ser consultada en *e-BERTONI*, el blog personal de Eduardo Bertoni, disponible en: http://bit.ly/1roLK0Y.

44 *Véase también*, Consejo Asesor de Google sobre el Derecho al Olvido, *Report of the Advisory Committee to Google on the Right to be Forgotten*, 2015, p. 4, disponible en: http://bit.ly/1r2Vv7e.

45 Naciones Unidas, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra* nota 20, pp. 5 y 6.

46 Intelligence Squared U.S., *"The U.S. should adopt the 'right to be forgotten' online"*, disponible en: http://bit.ly/1FOJDcW.

47 TJUE, *supra* nota 38, párrafo 81.

su derecho a la privacidad por esos contenidos y pide al buscador ser 'desindexada'] prevalecen igualmente, con carácter general, sobre el mencionado interés de los internautas".

A la hora de pensar en legislación en Argentina hay que tener en cuenta las particularidades y diferencias entre el marco europeo de protección de datos personales y el sistema interamericano de protección de derechos y su robusto hincapié en el fortalecimiento del derecho a la libre expresión. Trasladar el abordaje europeo al marco regulatorio argentino (y de América Latina, en general) por ejemplo, podría entrar en conflicto con la prohibición de censura previa contemplada en el artículo 13 de la Convención Interamericana sobre Derechos Humanos.[48] Si bien excede los objetivos de este trabajo, es un tema a tener en cuenta y que merece un análisis en profundidad a la hora de pensar en regulación en la materia.

- **Herramienta de censura en manos de privados.** Esta es de las cuestiones más preocupantes de la decisión del tribunal europeo. L*a persona interesada en* eliminar un enlace de un buscador, según el fallo, puede presentar esas solicitudes directamente al gestor del motor de búsqueda que deberá entonces examinar debidamente si son fundadas.[49] Es decir, esta "solución" deja en manos de actores privados –de Google y del resto de los buscadores– la decisión final sobre a qué información y a qué contenidos podemos acceder en internet. Una compañía termina ejerciendo un rol judicial[50] y ni los usuarios ni los generadores del contenido son consultadas/os.[51]

- **Desincentivos económicos y en desmedro de los intermediarios más "pequeños".** Este tipo de decisiones parecen difíciles de implementar para las empresas más pequeñas que actúan como intermediarios. A todas luces, una compañía como Google puede destinar tiempo y

---

48 OEA, *Convención Americana sobre Derechos Humanos*, 1969, artículo 13, disponible en: http://bit.ly/1KnISi7.

49 "El gestor de un motor de búsqueda en Internet es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas web publicadas por terceros". TJUE, comunicado de prensa nº 70/14, 13 de mayo de 2014, disponible en: http://bit.ly/1iMTO8N.

50 *Véase*, Bernal, P. A., *supra* nota 37, p. 18.

51 Floridi, Luciano, "*Right to be forgotten: who may exercise power, over which kind of information?*", en: The Guardian, 21 de octubre, disponible en: http://bit.ly/1nyUbIG. *Véase también,* Consejo Asesor de Google sobre el Derecho al Olvido, *supra* nota 44, p. 17.

dinero a revisar los pedidos de desindexación. Pero, ¿qué ocurre si este tipo de decisiones obligan también a generadores de contenidos, otros buscadores y plataformas que no cuentan ni con los recursos ni el *staff* de asesores legales que las compañías más poderosas?

Como dijimos antes, el manejo de los datos personales y la privacidad en entornos digitales son cuestiones clave que merecen la debida atención y la búsqueda de soluciones balanceadas con respecto al ejercicio de otros derechos humanos fundamentales. El llamado derecho al olvido en los términos del fallo del tribunal europeo, desde nuestra perspectiva, aparece como una mala solución, extrema, para un problema tan complejo.

Como señala Carlos Cortés Castillo en su trabajo sobre el tema, este escenario obliga a buscar otras interpretaciones y otras posibles soluciones que apunten a mayor expresión y ejercicio de derechos, y no menos.[52]

Y en la resolución de este "problema", como vimos a lo largo de este trabajo, los buscadores –y los intermediarios en general– tienen un rol clave. Son, en gran medida, quienes "resuelven" el problema. Incluso, con el riesgo de actuar como censores. En este sentido, y como expresamos en secciones anteriores, poner en manos del intermediario la decisión sobre si desindexar resultados de búsqueda, o no, a pedido de los usuarios, los pone en un rol de mucho poder. Y, si tenemos en cuenta que pueden enfrentarse a responsabilidad en caso de incumplir con las peticiones, los intermediarios querrán evitar ese riesgo, y podrían transformarse en censores.

III. Conclusiones y recomendaciones

A los fines de respetar los derechos humanos en internet, cualquier proyecto de legislación sobre responsabilidad de intermediarios, o derecho al olvido, debería:

- En principio, abordar –dada la complejidad de estos temas– la responsabilidad de los intermediarios mediante una regulación específica y no a través de marcos legales generales.
- No trasladar "soluciones" aplicadas en otros contextos a los proyectos de ley locales. La regulación de internet debería discutirse a la luz del

[52] Cortés Castillo, Carlos, *supra* nota 3, p. 148.

marco establecido por el sistema interamericano de protección de derechos de derechos humanos.

- Asegurar que las decisiones sobre desindexación, bloqueo y remoción de contenidos estén en manos de una autoridad judicial, y no de actores privados.
- Adoptar un régimen que otorgue inmunidad a los intermediarios por contenidos generados por terceros y establezca que solo deben obedecer a órdenes de remoción o filtrado de contenidos emanadas de una autoridad judicial. El intermediario podrá ser responsable si incumple dicha orden, pero nunca debe ser responsabilizado por el contenido en sí –salvo que haya modificado o intervenido dicho contenido–.

La "internet de las cosas": más internet que otra cosa

Carlos Cortés Castillo[1]

Resumen

El objetivo de este documento es ofrecer un panorama sobre el tema conocido públicamente como *internet de las cosas* (IoT). Primero, plantea el antecedente histórico de la computación ubicua; segundo, describe los retos técnicos que implica hablar de una internet de las cosas; tercero, habla sobre los riesgos de un entorno de objetos interconectados.

La idea subyacente de este texto es que internet de las cosas reúne una amalgama de conceptos e ideas sobre productos y servicios presentes y futuros. Es decir, gira alrededor de hechos, ideas y meras especulaciones. Esto implica, en parte, que cualquier aproximación a la internet de las cosas pasa por debates conocidos sobre internet, privacidad y seguridad en línea, entre otros.

I. Introducción

De un tiempo para acá venimos oyendo hablar de un nuevo amanecer en la tecnología: internet de las cosas. Un mundo de objetos interconectados, de ciudades y hogares inteligentes, de aplicaciones y servicios automáticos. Los ejemplos de este futuro digital son tan inagotables como la imaginación de sus exponentes. Los más convencionales se relacionan con el hogar: cortinas que interpretan la luz del día para abrirse o cerrarse, lavadoras que pueden

[1] Este documento fue elaborado por Carlos Cortés Castillo, investigador del iLei en el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. Actualmente, es Public Policy Manager en Twitter. La investigación contó con el apoyo de Juan Diego Castañeda y aportes de Eduardo Bertoni, director del CELE.

interactuar con la ropa para reportar su estado de desgaste, y neveras que reportan directamente los alimentos que están por caducar o que hacen falta.

También hay ejemplos más complejos, que involucran un mayor grado de interacción entre la persona y la máquina, y entre éstos y los entornos sociales: un profesor se encuentra enfermo y avisa a la universidad donde trabaja que no se presentará a clase. La universidad envía esa información a los estudiantes y, a través de un sistema que integra dispositivos conectados a la red, cambia la agenda de los estudiantes, cambia la hora de sus despertadores e incluso programa la cafetera para una hora más tarde.[2]

En esencia, internet de las cosas promete escenarios donde los objetos facilitarán nuestra vida cotidiana. Pero, ¿es realmente algo distinto a lo que ya tenemos? ¿Es la internet de las cosas una idea, un proyecto, una estrategia comercial? ¿Conlleva riesgos?

Parece prematuro adentrarse en esta discusión cuando todavía internet es una tecnología joven y su desarrollo y regulación enfrentan tantas incertidumbres. Más aún en América Latina, donde la penetración ni siquiera alcanza el 50% y las computadoras portátiles y los teléfonos móviles siguen siendo artículos costosos.[3] Sin embargo, la atención que los medios de comunicación vienen prestándole al tema y la inclinación de la gente por consumir innovación tecnológica –ya sea a manera de noticias o de productos como tal–, amerita hacer una revisión más desapasionada.

El objetivo de este documento es entonces ofrecer un panorama sobre el tema conocido públicamente como internet de las cosas. Para hacerlo, primero plantearemos el antecedente histórico de la computación ubicua, lo cual permite ubicarse de mejor manera en la coyuntura actual; en seguida, describiremos los retos técnicos que implica hablar de una internet de las cosas; en tercer lugar, describiremos los riesgos de un entorno de objetos interconectados –haciendo énfasis en el acopio de información y los problemas de seguridad–; y, finalmente, plantearemos conclusiones y recomendaciones.

La idea subyacente de este texto es que internet de las cosas reúne una amalgama de conceptos e ideas sobre productos y servicios presentes y futuros. Es decir, gira alrededor de hechos, ideas y meras especulaciones. Esto implica, en parte, que cualquier aproximación a la internet de las cosas pasa por debates conocidos sobre internet, privacidad y seguridad en línea, entre

---

2 *Véase*, *Internet of Things Europe, Teaser N. 1: Student* en: *Digital Agenda EU,* disponible en: http://bit.ly/1krMxiQ, último acceso: 30 de noviembre de 2014.

3 *Véase,* “*Internet Usage Statistics for all the Americas”,* en: *Internet World Stats,* disponible en: http://bit.ly/1fOzBhb, última consulta: 30 de noviembre de 2014.

otros. Para efectos de discusiones sobre regulación y políticas públicas de internet, esta claridad puede servir para evitar distraer la atención o, más bien, para centrar la atención en los aspectos relevantes de este tema.

II. La sala de trabajo del futuro

En septiembre de 1991, Mark Weiser escribió para *Scientific American* un artículo titulado “El computador para el siglo XXI”. En una de las fotos que acompañan el texto aparecen Weiser y tres personas más en una especie de sala de trabajo del futuro. La primera está parada explicando algo en una pantalla o televisor gigante, similar en tamaño a un tablero de un salón de clases. Las demás están cómodamente sentadas alrededor de una mesa redonda: dos de ellas trabajan en tabletas monocromáticas –en verde y negro– con lápices o bolígrafos en la mano, mientras que la última –Weiser– observa un monitor individual.[4]

Se trataba, en realidad, de un futuro próximo. Para entonces este grupo de científicos del centro de investigación de Xerox en Palo Alto (conocido como PARC, por su nombre en inglés) ya había diseñado tres dispositivos, dos de los cuales aparecen en la foto: los *tabs*, pequeños aparatos que hacían las veces de notas *Post–it*; los *pads,* que se asemejaban a una libreta u hoja de papel; y los tableros, homónimos de sus pares analógicos. Weiser proponía que la oficina del futuro tuviera centenares de estos en una habitación. Y, contrario a lo que vemos hoy, no se trataba de dispositivos personales. De la misma forma como una persona usa una hoja de borrador en una reunión, la idea era que pudiera usar un *tab* o *pad* cualquiera que estuviera disponible, para después transmitir la información sin llevárselo.

Aunque en 1991 se trataba de una escena que maravillaría a una persona común y corriente, el PARC veía todos estos aparatos como una escala para llegar a algo más grande. Para Weiser, la noción del computador personal era en sí misma equivocada:

> Tales máquinas no pueden lograr que la computación sea una parte integral e invisible en la forma como la gente vive sus vidas. Por lo tanto, estamos tratando de concebir una nueva forma de pensar acerca de las computadoras en el mundo, una que tome en cuenta el medio ambiente natural del ser humano y permita que las computadoras como tales desaparezcan en un segundo plano.[5]

---

4 La fotografía puede verse en: http://bit.ly/2069IwU, última consulta: 30 de noviembre de 2014.
5 Weiser, Mark, *“The Computer of the 21st Century”*, en: *Scientific American*, Irvine, Universidad

Dicho en otras palabras, Weiser abogaba porque el poder de la computación se liberara de la esclavitud de la pantalla. Solo así podría mezclarse en nuestras vidas cotidianas.

Weiser –que moriría en 1999 sin llegar a ver la revolución que vaticinó– bautizó esta compenetración entre la máquina y el entorno humano como "computación ubicua", que para él no podía entenderse ni como realidad virtual ni inteligencia artificial. Esta última se enfoca en simular el mundo real, y no en aumentar y mejorar el que ya existe. Tampoco se trataba de lo primero. El reto, concluía, era incrustar la computación en el día a día de las personas. Para la época del artículo de *Scientific American* los *switchs* de luz, termostatos, hornos y equipos de sonido ya tenía algún nivel de computación interna. El propósito era, entonces, que esos y otros objetos comenzaran a formar parte de una red omnipresente e invisible.

Esta proposición se adentra en los terrenos del diseño, donde quizá el exponente más relevante para los partidarios de la computación ubicua es el diseñador japonés Naoto Fukusawa. Fukusawa considera que los productos deben ser sensibles a la naturaleza humana; deben poder usarse "sin pensar". Cuando los objetos se amoldan de manera natural a ciertos ambientes y ciertos patrones de uso, se disuelven en la acción del individuo –"diseño que se disuelve en conducta"[6]–. Un *ethos* similar guiaba a Steve Jobs, el fundador de Apple, para quien los objetos tenían una esencia y una pureza intrínseca.[7] Weiser resumió ese horizonte en una frase que a la postre se convirtió en el prólogo de la computación ubicua, el antecedente obligatorio –y técnicamente más ajustado– de lo que hoy conocemos como internet de las cosas (*Internet of Things* o IoT): "Las tecnologías más profundas son aquellas que desaparecen. Se tejen a sí mismas en la tela de la vida diaria hasta que son imposibles de distinguirse de esta".[8]

Distintos autores han propuesto nuevas aproximaciones que abarquen y den un sentido integral a la idea de computación ubicua.[9] Al final, cada apor-

---

de Californa Irvin, 1991, p. 94. Traducción propia.

6 *Véase,* Parsons, Tim, *Thinking Objects: Contemporary Approaches to Product Design*, Lausana, AVA Book, 2009.

7 *Véase,* Morozov, Evgeny. "*Steve Jobs's pursuit of perfection—and the consequences*", en *The New Republic*, febrero de 2012, disponible en: http://bit.ly/1RYhzgC, última consulta: 30 de noviembre de 2014.

8 *Ibíd.*

9 *Véanse,* Bell, Genevieve, Dourish, Paul, "*Yesterday's tomorrows: notes on ubiquitous computing's dominant vision*", en *Personal and Ubiquitous Computing,* abril 2006; Abowd, Gregory, Mynatt, Elizabeth, "*Charting past, present, and future research in ubiquitous computing*", ACM Transactions on Computer–Human Interaction (TOCHI), julio 2000; Hansmann, Uwe

te da un elemento adicional sin que parezca posible asir algo tan amplio y ambiguo. Adam Greenberg, por ejemplo, considera que definir la computación del futuro como aquella que es móvil, usable, conectada o situada, ofrece una visión muy angosta del fenómeno. En respuesta, él propone el paradigma del *everyware,* un neologismo en inglés que mezcla términos como “todos los días” (*everyday*) y “en todas partes” (*everywhere*), con otros como “ubicado”, “consciente” (*aware*) y “usable” (*wearable*). *Everyware,* según Greenberg, es una experiencia que involucra “una ecología diversa de dispositivos y plataformas” que difiere del entendimiento convencional que tenemos sobre las computadoras. Se trata de un fenómeno distribuido: el poder y significado no radican en los nodos sino en la red, que es en efecto invisible y que permea lugares y actividades.[10]

La descentralización y dispersión de dispositivos implica una multiplicación de las fuentes de información. Información que no necesariamente tiene que procesar un computador de uso general, sino que está presente en los mismos objetos, que dan cuenta del lugar en el que se encuentran y la función que cumplen; objetos conscientes de su contexto (*context–aware*). Kevin Ashton, la persona que acuñó el término de “internet de las cosas”, considera que el núcleo es dotar a los objetos con la capacidad de recoger información por ellos mismos y no a través de seres humanos, como hoy se hace.[11]

Reuniendo de una u otra forma los elementos anteriores, se han propuesto decenas de definiciones del IoT. Para efectos de ilustración, citaremos dos:

- “Es una infraestructura global interconectada, enlazando objetos físicos y virtuales a través de la explotación de la captura de datos y las capacidades de comunicación. Ofrecerá identificación específica de objetos y capacidades sensoriales y de conectividad como la base para el desarrollo de servicios cooperativos y aplicaciones independientes”.[12]

---

y otros, *Pervasive computing: The mobile world*, Springer, 2003; Saha, Debahis, Mukherjee, Amitava, *Pervasive computing: a paradigm for the 21st century,* IEEE Computer, marzo 2003, pp. 25-31.

10 *Véase,* Greenfield, Adam, *Everyware. The dawning age of ubiquitous computing*, San Francisco, New Riders, 2006, p. 38-39.

11 Ashton, Kevin, “That ‘Internet of Things’ Thing”, en: RFID Journal, Hauppauge, junio de 2009, disponible en: http://bit.ly/1bt4GBP, última consulta: 30 de noviembre de 2014.

12 CASAGRAS, “*RFID and the Inclusive Model for the Internet of Things*”, citado en: “Internet of Things Definitions. Postscapes”, disponible en: http://bit.ly/10mOfrW, última consulta: 30 de noviembre de 2014. Traducción propia.

- “Un mundo donde los objetos están integrados de manera perfecta y sin sobresaltos en la red de la información, y donde los objetos físicos pueden convertirse en participantes activos de los procesos comerciales. Los servicios pueden interactuar con estos ‘objetos inteligentes’ a través de internet, hacer una consulta y cambiar su estado y cualquier información asociada con ellos”.[13]

Internet de las cosas se plantea también como una fase evolutiva en la relación en línea entre el individuo y la computadora. Servicios como el correo electrónico, los mensajes de textos y las llamadas, tenían el propósito de satisfacer una interacción de persona a persona. En efecto, en una primera etapa de internet la mayor parte del tráfico correspondía a datos de voz y texto. Más adelante, apareció la interacción individuo–máquina con servicios de distribución de contenido –como el video por demanda–, que hoy ocupan un lugar protagónico. Ahora, con la computación ubicua en el horizonte, los servicios de automatización plantean una relación máquina–máquina o cosa–cosa (dispositivos que “hablan” entre sí: sensores de movimiento o de luz que envían una orden a un sistema de sonido o de seguridad, o automóviles que capturan datos de las autopistas).[14]

Más allá de eso, hoy por hoy el énfasis del debate público sobre la IoT parece estar más en el diseño y estética de la cosa, que en la computación que requiere. David Rose se refiere a los “objetos encantados”, que empiezan como algo ordinario –un zapato, una billetera, un bombillo– para convertirse en aparatos extraordinarios gracias a los sensores, conexiones y procesos tecnológicos incrustados. Es ahí donde encontramos las imágenes futuristas, ya no desde la visión remota de Weiser sino desde un mañana que parece cercano. Parece, decimos, porque muchos de los anuncios de internet de las cosas dependen de posibilidades tecnológicas y realidades de mercado. Es decir, la internet de las cosas está y no está entre nosotros.

III. Los retos técnicos del IoT

La computación ubicua que imaginaba Weiser implicaba superar varios escollos que él mismo dejó planteados. En primer lugar, el problema del

---

13 Haller, Stephan, “*Internet of Things: An Integral Part of the Future Internet*”, SAP Research, mayo 2009, disponible en: http://bit.ly/1NOE3ce, ultima consulta: 30 de noviembre de 2014.

14 *Véase,* Chaouchi, Hakima (ed.), *The Internet of Things: Connecting Objects to the Web,* Wiley, 2010.

movimiento de dispositivos: “Los ingenieros tendrán que desarrollar nuevos protocolos de comunicación que reconozcan explícitamente el concepto de máquinas que se mueven en el espacio físico”[15]. En segundo lugar, la interconexión de las redes y la interoperabilidad de los sistemas. En 1991 ya existían redes cerradas –tanto cableadas como inalámbricas– para la transmisión de datos. Además, la capacidad estaba en incremento, especialmente en distancias cortas. Pero un dispositivo no podía tener simultáneamente conexión inalámbrica de muy corto alcance, inalámbricas de largo alcance, y fijas de alta velocidad. Finalmente, se necesitaría un método que permitiera un verdadero intercambio de datos. Ahí el científico del PARC se aventuró con una predicción: las redes del futuro usualmente no dedicarán su ancho de banda a una sola transmisión; *“*en cambio, permitirán que una enorme cantidad de transmisiones de baja velocidad se lleven a cabo de manera simultánea”.[16]

No hacen falta más pistas. Weiser marcaba un derrotero –en el que por supuesto participaron miles de personas como él– para llegar a lo que hoy tenemos: conexiones de datos celulares, conexiones inalámbricas como *Wifi* y *Bluetooth,* y la conmutación de paquetes.[17] Estos avances técnicos, sumados a los microprocesadores y los sensores para identificar objetos, permiten imaginar la internet de las cosas.[18]

Las Etiquetas de Identificación por Radiofrecuencia (RFID, por su nombre en inglés) son un elemento básico en este sistema descentralizado de datos. Pueden ser tan pequeñas como el botón de una camisa o un grano de arroz, y están compuestas por dos partes: un “transpondedor”, que contiene un microchip y una antena, y un lector, que activa y recupera la información que aquel almacena.[19] En otras palabras, las etiquetas RFID guardan datos y los transmiten vía radio, a través de una antena, a un dispositivo con capacidad de leerlos.

Estas etiquetas pueden ser pasivas, semipasivas o activas. Como su nombre lo indica, las pasivas no tienen alimentación eléctrica propia, sino que se

---

15 *Ibíd.*, p. 101. Traducción propia.

16 *Ibíd.*

17 Sobre la conmutación de paquetes, *véanse* Cortés, Carlos. “La neutralidad de la red: la tensión entre la no discriminación y la gestión” y “Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet”, en: Bertoni, Eduardo (comp.) *Internet y derechos humanos. Aportes para la discusión en América Latina,* Buenos Aires, CELE - Universidad de Palermo, 2014, disponible en: http://bit.ly/NVQ5K5.

18 *Véase,* Kellmereit, Daniel, Obodovski, Daniel, *The Silent Intelligence: The Internet of Things,* San Diego, DnD Ventures. 2013.

19 *Véase,* Finkenzeller, Klaus, *RFID Handbook. Fundamentals and applications in contactless smart cards and identification*, segunda edición, Chippenham, Wiley, 2003, p.7.

activan gracias a la energía que produce la señal del lector. Las semipasivas, mientras tanto, usan batería para alimentar el microchip y la energía del lector para hacer la transmisión. Finalmente, las etiquetas activas emplean una batería capaz de alimentar tanto el microchip como la transmisión de la señal.[20]

Usualmente, las etiquetas RFID contienen datos sobre la identidad del objeto, conocida como código electrónico de producto (EPC, por su nombre en inglés). Así, es usual ver estas etiquetas en almacenes de cadena adheridas a ropa, juguetes o electrodomésticos. En ese contexto, cumplen una función similar, pero más sofisticada, que la del código de barras. La tecnología RFID se emplea también en industrias como la automotriz, donde es posible monitorear el progreso del ensamblaje de las partes; en la de alimentos, para monitorear inventarios, y en la farmacéutica, para identificar medicamentos y fechas de caducidad. Igualmente, las etiquetas RFID pueden "inyectarse" en animales para efectos de identificación –recientemente, Eduardo Bertoni contaba sobre un proyecto en Argentina para monitorear el ganado en el país con propósitos tributarios–,[21] o adherirse a dispositivos médicos, como el marcapasos, para monitorear su funcionamiento y el estado de salud del paciente.

La tecnología RFID, sin embargo, no resulta suficiente para que los escenarios más ambiciosos del IoT sean una realidad. La Agenda Digital de la Unión Europea plantea el siguiente ejemplo de internet de las cosas: una persona ha sufrido un accidente en su automóvil y automáticamente se envía una alerta a un hospital cercano. Esta alerta, además, sirve como notificación para que los otros automóviles informen a sus conductores sobre el hecho y la necesidad de tomar una ruta alterna.[22]

Tal nivel de comunicación entre objetos no se lograría con etiquetas RFID, puesto que involucra acciones más complejas: el automóvil debe tener sensores para determinar su posición (giroscopios) y para darse cuenta de que se detuvo de manera abrupta (acelerómetros). También debe contar con alguna capacidad para conectarse a internet y enviar un mensaje de emergencia. De la misma forma, los automóviles que van en la vía deben poder recibir a través de internet la sugerencia de desvío, todo lo cual debe estar mediado por algún tipo de central de tráfico.

---

20 *Véase,* Atzori, Luigi, Iera, Antonio, y Morabito, Giacomo, *The internet of things: A survey,* en: *Computer networks,* 54.15, junio 2010, p.2790.

21 Bertoni, Eduardo, "El derecho a la privacidad de las vacas", en: eBertoni, agosto de 2014, disponible en: http://bit.ly/20mQDfk, última consulta:4 de diciembre de 2014.

22 *Véase, Internet of Things Europe – Teaser N° 3: Traffic,* en: *Digital Agenda EU,* disponible en: http://bit.ly/1XOwRF5, última consulta: 30 de noviembre de 2014.

Esta situación plantea un contraste entre las etiquetas RFID y un “objeto inteligente”, que en última instancia sería necesario para la IoT –al menos en los términos en que se vende comercialmente–. Para hablar de internet de las cosas se requiere de objetos que puedan comunicarse entre sí, den cuenta de su entorno y, en ocasiones, actúen sobre él.[23] Un objeto es “inteligente” dependiendo de sus niveles de (i) “conciencia” sobre el ambiente, (ii) representación, que es la forma como se comporta, y (iii) capacidad de interacción con el usuario.[24] De allí se colige que un objeto con un sensor RFID adherido puede contener datos de manera descentralizada –siguiendo la idea del *everyware*–, pero no puede hacer parte de un entorno digital ubicuo.

Esto significa que si los “objetos inteligentes” pretenden ser autónomos, y realmente descentralizados, deberán tener la capacidad funcional para cumplir con los protocolos de la red. De lo contrario, serán simplemente apéndices de máquinas más grandes. Dicho de otra forma, la “internet” en la internet de las cosas es la misma que conocemos, y si los “objetos inteligentes” van a formar parte de esta red, tendrán que ser compatibles.[25] Jean–Phillipe Vasseur y Adam Dunkels consideran que, por su flexibilidad, el protocolo TCP/IP es apropiado para una red de “objetos inteligentes”. Mientras que un protocolo semicerrado o propietario afectaría la escala de dispositivos conectados, el TCP/IP busca un “óptimo global”, es decir, una mayor compatibilidad e interconexión.

Para que una serie de datos puedan ir de un lugar a otro se requiere que tanto el receptor como el emisor estén identificados y que esa identificación no se confunda con otras. El protocolo de internet (IP) cumple esa función al asignar direcciones únicas a cada uno de los nodos que se conectan a la red –ya sea un computador, un teléfono o un radio–. La versión 4 del protocolo de internet IP es la más extendida hoy (IPv4). Dado que su tamaño es de 32 bits,[26] permite unas 5 000 millones de direcciones únicas, las cuales no

---

23 *Véase,* Vasseur, Jean-Philippe, Dunkels, Adam, *Interconnecting smart objects with ip: The next internet,* Burlington, Morgan Kaufmann, 2010, p.3-7. *Véase también,* Cristea, Valentin, Dobre, Ciprian, y Pop, Florin, “*Context–aware environments for the Internet of things*” en: Bessis, Nik, y otros (eds.), *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*, Springer Berlin Heidelberg, 2013. p. 26.

24 Kortuem, Gerd, y otros, “*Smart Objects as Building Blocks for the Internet of Things*”*,* en: *IEEE Internet Computing,* 14.1, 2010, p.45.

25 *Véase,* Vasseur, Jean-Philippe, Dunkels, Adam, *supra* nota 23, p. 28. Para una explicación sobre la arquitectura de internet, *véase*, Cortés, Carlos, *supra* nota 17.

26 Un bit es la unidad básica de información digital. Puede tener sólo uno de dos valores: 0 o 1. Cuando se habla de una dirección de 32 bits se hace referencia a su tamaño pues, en este caso, ella tiene 2^32 combinaciones diferentes posibles.

son suficientes para los 50 000 millones de dispositivos que, según empresas como Cisco, estarán conectados a internet para 2020.[27] Por ello, se ha diseñado la versión 6 del protocolo (IPv6), que cuenta con un enorme número de direcciones ya que su tamaño asciende a 128 bits.[28]

Si en gobernanza de internet se identificaba como un problema la gestión de recursos críticos de internet y, en especial, el agotamiento de direcciones IP –y, por lo tanto, la necesidad de hacer la transición de IPv4 a IPv6–, internet de las cosas hace aún más patente esa necesidad.

Este no es el único escollo técnico que presenta la IoT. Alrededor de los propósitos de conectividad e interoperabilidad, y de las capacidades de los dispositivos, se dan toda suerte de discusiones entre ingenieros. Por ejemplo, en una red de "objetos inteligentes" el tráfico de datos tendrá que determinarse según la capacidad de los nodos, ya que las cosas conectadas no tendrán ni la memoria ni la energía de una computadora tradicional. Igualmente, es necesario adoptar un protocolo de transporte de datos (TCP o UDP), y adoptar decisiones metodológicas para que los objetos puedan conectarse a la red. Hoy contamos con protocolos como SLP, UPnP (*Universal Plug and Play*) y Zeroconf, que permiten que un periférico conectado a una red –una impresora, un control para juegos, un ratón– sea reconocido inmediatamente y quede establecida la comunicación.

Por último, los "objetos inteligentes" tendrán que cumplir ciertos requisitos de seguridad: confidencialidad de los datos que almacenan y envían, integridad de la información, protección del usuario legítimo y prevención de fraude. Una serie de riesgos que no distan demasiado de los que subsisten hoy en sistemas de información y computadoras. A este punto nos referiremos brevemente en el siguiente apartado.

IV. El riesgo de un entorno digital omnipresente

Para no pocos críticos, la idea de tener objetos que registren y reporten todos nuestros movimientos y actividades constituye *"una irrupción tecnológica violenta en la vida cotidiana"*[29]. No hay que ir demasiado lejos para

---

27 IETF, "RFC791*"*, disponible en: http://bit.ly/1QEYWLA.

28 *Véase,* Coffeen, Tom, *IPv6 Address Planning. Designing and Address Plan for the Future*, O'Reilly Media, 2014.

29 Araya, Agustín, "*Questioning Ubiquitous Computing*", en: *Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science,* ACM Press, 1995. Para consultar críticas similares, *véase*, Bohn, Jürgen, "*Social, Economic, and Ethical Implications of Ambient Intelligence and*

entender la preocupación: en la propia visión de una red omnipresente de objetos y dispositivos subyace un sistema robusto de vigilancia del individuo. No necesariamente uno público o arbitrario pero, aun así, inquietante.

Sin tener que adentrarse en el terreno de la internet de las cosas, esta cuestión subsiste hoy en día en el entorno digital de computadores y teléfonos móviles. Con la tecnología de la que disponemos, es posible monitorear comunicaciones y movimientos en tiempo real. Por supuesto, en un contexto en el que todos los objetos almacenan datos sobre el individuo o que posibilitan su identificación o ubicación, la capacidad de vigilancia solo aumenta. De una parte, será más fácil monitorear y, de la otra, habrá más datos personales para procesar.

En muchos casos, el primer actor interesado en esa información será el Estado. "Todos esos nuevos objetos en línea son un tesoro de datos si usted es una 'persona de interés' para la comunidad espía"[30], afirma David Petraeus, exdirector de la Agencia Central de Inteligencia de Estados Unidos. "Con el surgimiento de la 'casa inteligente', cuando usted use en su '*smartphone*' la aplicación para ajustar la luz de su sala, estará enviando datos etiquetados y geolocalizados que una agencia de espionaje podrá interceptar en tiempo real".[31]

De la misma forma como hoy las conversaciones y los datos son interceptados, los objetos inteligentes de una casa, una ciudad o una fábrica serán usados como fuente de información. Y de la misma forma en que el IoT se acoplará a la vida cotidiana por su ubicuidad e invisibilidad, los esquemas de vigilancia terminarán siendo omnipresentes e imperceptibles. Lawrence Lessig hace un interesante paralelo entre las capacidades de vigilancia de las nuevas tecnologías y el referente paradigmático descrito en *1984*, la novela distópica de George Orwell. Mientras que en este último existía la "telepantalla", un aparato transparente e imperfecto, ya que era posible saber en dónde y en qué condiciones observaba, los dispositivos conectados a internet ofrecen formas subrepticias de monitoreo y control.[32]

Ubiquitous Computing", en: Weber, Werner, Rabaey, Jan, y Aarts, Emile, *Ambient Intelligence*, Springer Berlin Heidelberg, 2005.

30 Ackerman. Spencer, "*CIA Chief: We'll Spy on You Through Your Dishwasher*", en: *Wired*, marzo de 2012, disponible en: http://bit.ly/1NOE5B6, última consulta: 30 de noviembre de 2014. Traducción propia.

31 *Ibíd.*

32 *Véase,* Lessig, Lawrence, "*On the Internet and the Benign Invasions of Nineteen Eighty-Four*", en: Gleason, Abbot, Goldsmith, Jack, y Nussbaum, Martha, *On Nineteen Eighty-Four. Orwell and our Future,* Princeton, Princeton University Press, 2005.

La captura masiva de información personal en tiempos de la IoT es distinta –y más preocupante– que la actual, por varias razones: primero, se capturará información en muchos lugares más; segundo, el acopio será invisible; tercero, los datos serán más íntimos –qué, dónde, cuándo, cómo, con quién, por cuánto tiempo, por qué–; y, cuarto: las facilidades de interconexión conllevarán a que nuestros datos sean compartidos en niveles nunca antes vistos.[33] Compárese, por ejemplo, la etiqueta RFID con el código de barras –su antecesor–: mientras el segundo contiene alguna información sobre el producto, la primera puede incluir datos personales e historiales de compra; mientras el segundo debe estar a la vista para capturar la información, la primera solo necesita de un lector a una distancia adecuada; y, mientras el segundo requiere de algún nivel de interacción humana, la primera opera entre máquinas.

Asociada a la invasión de la privacidad –entendiéndola en un sentido que va más allá de la protección de un espacio íntimo– la IoT conlleva también un riesgo de normalización del individuo y de coerción de su autodeterminación. Para Greenfield, el éxito del *everyware* –que, recordemos, es esa intersección entre ubicuidad y cotidianidad– depende de que el ecosistema de objetos pueda moldearse a la vida de una persona de manera tal que interprete y distinga entre órdenes o simple ruido, entre acciones relevantes e irrelevantes.[34] En otras palabras, el IoT tiene que ser tan preciso y previsible como el algoritmo de un programa. ¿Qué nivel de autodeterminación y espontaneidad quedaría para el individuo?

Natasha Dow-Schüll, quien estudió la compleja relación entre los apostadores y las máquinas tragamonedas en Las Vegas, plantea que los procesos de automatización en la relación individuo-máquina van desplazando el núcleo de control de la actividad –y, por ende, la capacidad de acción–[35] del primero al segundo. La persona comienza a participar en acciones en las que responde automáticamente, perdiendo de alguna forma el sentido de sí misma.[36] Siguiendo esa línea, Bruce Sterling considera que en la IoT el usuario no decide ni entiende ni modifica; son las grandes empresas –cuyas prioridades son comerciales– las que determinan cómo y qué se conecta.[37]

---

33 *Véase,* Lahlou, Saadi, Langheinrich , Marc, Röcker, Carsten, "*Privacy and trust issues with invisible computers*", en: *Communications of the ACM*, 48.3, 2005, p.59.

34 *Véase,* Greenfield, Adam, *supra* nota 10.

35 En inglés se utiliza el término *agency.* Acá lo traducimos como capacidad de acción, a pesar de que el significado es un poco más complejo.

36 *Véase,* Dow Schüll, Natasha, *Addiction by Design: Machine Gambling in Las Vegas*, Princenton, Princenton University Press, 2014.

37 *Véase,* Sterling, Bruce, *The Epic Struggle of the Internet of Things*, Moscú, Strelka Press, 2014.

Un ecosistema “exitoso” de IoT podría desembocar entonces en lo que se conoce como una “arquitectura de control”, una configuración que define o moldea de manera muy detallada el tipo de conductas permitidas. Y aunque es posible que ese no sea el objetivo de muchos de sus proponentes, resulta claro que es útil para ese fin. Los sensores para identificar usuarios, bienes o servicios de ubicación, se prestan fácilmente para fines de control y supervisión.[38] Desde una perspectiva comercial, pueden ser herramientas ventajosas para el individuo; desde una perspectiva policial, se vuelven barreras, exclusas y cuellos de botella. Lessig considera que ante el control creciente en el entorno digital –invisible y preestablecido– el ser humano termina siguiendo un “principio bovino”: simplemente se ajusta a las cercas que ve, como las vacas.[39]

A continuación mencionamos más en detalle dos riesgos planteado acá entrelíneas: la acumulación masiva de información (el *big data*) y los riesgos de seguridad, inherentes a cualquier sistema de información y con opciones de escalar en el contexto de la IoT.

1. ‘Big data’

El *big data* es una herramienta que busca abarcar un conjunto de datos relevantes tan aproximado a la totalidad como sea posible. Es de alguna forma una paradoja: la captura y procesamiento de una infinidad de datos que se acerque al límite disponible. Su esencia se opone a una toma de muestra: el *big data* no analiza el préstamo de materiales de una biblioteca en particular, sino todos los préstamos, en todas las categorías y temas; no analiza un mensaje con palabras clave, sino que procesa todo el historial de conversaciones. Igualmente, para el *big data* lo relevante no es el porqué sino el qué. Averiguar por qué prolifera la gripe en ciertos lugares de un país es menos importante que detectar posibles casos de gripe a partir de búsquedas en Google.[40]

Para Kevin Ashton, el complemento entre el *big data* y la internet de las cosas es ideal: “si tuviéramos computadoras que supieran todo lo que hay que saber acerca de las cosas –usando datos que ellas mismas hayan recogido sin intervención humana– podríamos monitorear e inventariar todo y reducir significativamente las pérdidas, desperdicios y costos”[41]. Sin embargo, la

---

38 *Véase,* Cohen, Julie, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012.

39 *Véase,* Lessig, Lawrence, *supra* nota 32.

40 *Véase,* Cohen, Julie, *supra* nota 38.

41 Ashton, Kevin, *supra* nota 11. Traducción propia.

relación entre los datos masivos y la IoT no es estructural. El primero no es consecuencia de la segundo. El problema, nuevamente, es que un entorno ubicuo interconectado potenciaría el procesamiento de datos disponibles. Entre más objetos reciban y transmitan información, más profundo será el pozo de datos. Un riesgo que para Ashton es más bien una ventaja.

Las ventajas de analizar vastas cantidades de datos para encontrar patrones y tomar decisiones, son innegables. A través del *big data* las empresas cuentan con una base racional que les permite identificar individuos para categorizarlos en grupos con otros similares.[42] Así, pueden hacer ofertas diferenciadas, productos para nichos específicos o seguimientos a compras previas. Los efectos benéficos no se quedarán solo en las empresas. Esta herramienta permitirá observar mejores correlaciones entre hábitos de consumo y efectos ambientales, lo que puede incentivar un consumo más consciente.[43]

En el área de la salud, por ejemplo, se prevé que el *big data* propiciará opciones de vida más saludables; permitirá proveer tratamientos más adecuados; orientará la selección del profesional con mejores capacidades para atender un caso; racionalizará los costos del sistema de salud, y permitirá una mayor innovación en los servicios.[44]

No obstante, esta amplia oferta informativa, sumada a la vulnerabilidad de las bases de datos –piénsese en contexto frágiles como los latinoamericanos– y a decisiones arbitrarias y erróneas, puede desembocar en violaciones a la privacidad y en prácticas discriminatorias.

Uno de los ejemplos más documentados frente a este problema está en los datos masivos y la información financiera. Con datos crediticios, antecedentes personales, ubicación geográfica e información de redes sociales, los bancos han lanzado productos bancarios que terminan por segregar ciertos grupos –afroamericanos, concretamente– o han calificado la calidad de un cliente a partir de inferencias equivocadas (si vive en cierta zona, frecuenta ciertos lugares o usa cierto lenguaje, puede no ser confiable).[45]

---

[42] *Véase,* Barocas, Solon, Selbst, Andrew, "*Big Data's Disparate Impact*", SSRN 2477899, 2014, disponible en: http://bit.ly/1r8Yufj, última consulta: 30 de noviembre de 2014.

[43] Anderson, Jana, Rainie, Lee, "*The Future of Big Data*", en: *Pew Research Center's Internet & American Life Project*, julio de 2012, disponible en: http://pewrsr.ch/1PSuLn8, última consulta: 30 de noviembre de 2014.

[44] Groves, Peter, y otros, *The "big data" revolution in healthcare. Accelerating value and innovation,* McKinsey & Company, 2013.

[45] *Véase,* Peña Gangadharan, Seeta, "*The Dangers of High–Tech Profiling Using Big Data"*, en: *New York Times*, 7 de agosto de 2014, disponible en: http://nyti.ms/1oGwr3n, última consulta: 26 de noviembre de 2014.

Dichas conclusiones son el resultado de una combinación algorítmica, pero su fundamento es una decisión humana, con lo cual el error se sistematiza y el análisis sesgado del *big data* se perpetúa. Por ejemplo, volviendo al tema de salud, en el Saint George’s Hospital Medical School de Londres se creó un programa para seleccionar aspirantes laborales basándose en un modelo de análisis de postulaciones decididas favorablemente en el pasado. Posteriormente, la Comisión de Igualdad Racial encontró que al menos 60 de las 2 000 postulaciones que se presentaban anualmente se habían rechazado por razones de género. A la postre, el programa simplemente replicaba las decisiones discriminatorias de quienes habían llevado a cabo los procesos de selección en el pasado, cuyos datos definieron los criterios para modelar el programa.[46]

Aunque planteábamos al comienzo que el *big data* no es un efecto atribuible únicamente a la internet de las cosas, sí existe una complementariedad que puede potenciar, en particular, el riesgo de discriminación. A medida que la información personal se acumule –financiera, social, económica– y se ate a ubicaciones y accesos en una ciudad o lugar, surgirán esquemas de restricciones, como si se tratara de un gigantesco club social donde la gente tiene permiso para moverse a partir de los privilegios que tenga. Estos “regímenes de autenticación”, donde cada acción debe estar previamente validada, no podrán ser cuestionados por el individuo, ya que estarán incrustados en los objetos.[47]

2. Seguridad

La seguridad de un sistema depende de su capacidad para, por un lado, responder a ataques externos y, por el otro, evitar daños al ambiente o a las personas.[48] En inglés se ha habla de *secure* y *safe* que, si bien en español sólo encuentran traducción en la palabra “seguro”, hacen alusión a dos formas distintas de seguridad. Para Dunkel y Vasseur, entretanto, la seguridad es confidencialidad, integridad y disponibilidad.[49]

46 *Véase,* Lowry, Stella, Macpherson, Gordon, “*A blot on the profession*”, British Medical Journal (Clinical research ed.), 296.6623, 1988.

47 *Véase,* Greenfield, Adam, *supra* nota 10. Para más información sobre los regímenes de autenticación, *véase,* Cohen, Julie, *supra* nota 38,

48 *Véase,* Axelrod, C. Warren, *Engineering Safe and Secure Software Systems*,Norwood, Artech House, 2012.

49 *Véase,* Vasseur, Jean-Phillipe, Dunkels, Adam, *supra* nota 23,

En todos los elementos de la internet de las cosas –objetos, sensores, actuadores y conectores– hay puntos de vulnerabilidad, y en cada caso la virtud de automatización es a la vez un talón de Aquiles. Las etiquetas RFID –que son por ahora la tecnología principal de identificación– sirven como ejemplo: teniendo en cuenta que se trata de identificadores únicos que pueden ser leídos sin intervención humana, un dispositivo no autorizado puede "escanear" los datos allí contenidos. De la misma forma, podría falsificarse una etiqueta RFID o engañar de otra forma al dispositivo-lector para que, por ejemplo, registre equivocadamente la salida o entrada de un producto en un inventario. En pocas palabras, los problemas pueden surgir por etiquetas auténticas que son registradas por lectores clandestinos o por etiquetas falsas que, de una u otra forma, engañan a lectores legítimos.[50]

La lista de problemas de estas etiquetas no termina ahí. También es posible bloquear un lector legítimo exponiéndolo a una cantidad tal de etiquetas que no pueda procesar ninguna –similar a un ataque de denegación de servicio *DDoS* en internet–;[51] se puede generar interferencia en el espectro electromagnético de modo que no pueda leerse ninguna etiqueta; se puede obtener información ilegítimamente empleando intermediarios clandestinos; o un lector clandestino puede monitorear la comunicación entre etiquetas y lectores legítimos.[52]

Una vez capturados los datos de la etiqueta, se abren todos los problemas de seguridad y privacidad.[53] Una lectura de los objetos que carga una persona pueden dar mucha información sobre ella: entre otros, los objetos que lleva consigo, sus afinidades –libros, música– o su estado de salud –medicinas o recetas médicas–. Así mismo, a través de las etiquetas sería posible seguir los movimientos de alguien.[54]

---

50 *Véase,* Juels, Ari, "*RFID security and privacy: A research survey*", en *IEEE Journal on Selected Areas in Communications*, N. 24(2), 2006, p.384.

51 El DDoS es un ataque con el propósito de que una máquina o recurso de red quede indisponible para sus usuarios. Los métodos varían pero en general el ataque consiste en hacer miles de solicitudes simultáneas a un servidor o servicio, desbordando la capacidad de la máquina de atenderlos o procesarlos.

52 *Véase,* Khoo, Benjamin, "*RFID as an enabler of the internet of things: issues of security and privacy*", en: *International Conference on Internet of Things (iThings/CPSCom),* Dalian, 2011.

53 Medaglia, Carlo Maria, Serbanati, Alexandru, "*An overview of privacy and security issues in the internet of things*", en: Giusto, Daniel, y otros, *The Internet of Things*. Nueva York, Springer New York, 2010, p.391.

54 *Véase,* Weber, Rolf, "*Internet of Things. New security and privacy challenges*", en: *Computer Law & Security Review*, 26.1, 2010, p.24.

No obstante, como veíamos en el apartado anterior, la IoT prometida está compuesta por “objetos inteligentes” conectados entre sí y a internet. En esa línea, la presencia en red de cualquier cosa, en cualquier parte, en cualquier momento, multiplicará los puntos de entrada y salida de información y, por lo tanto, aumentará el riesgo. La heterogeneidad de los objetos conectados también ofrecerá niveles distintos de fragilidad. En otras palabras, no habrá soluciones que se ajusten –literalmente– a todos los tamaños del riesgo.[55]

Muchos de los ejemplos del peligro que representan los objetos conectados a internet suelen ser apocalípticos, tan radicales como los que desde la orilla opuesta se proponen como el idilio de la IoT. No obstante, en algunos de ellos es posible entrever el reto que enfrenta la industria, los gobiernos y la sociedad civil en este proyecto.

En 2013, Dick Cheney, exvicepresidente de la administración de George W. Bush, contó a la prensa que sus médicos le habían recomendado desactivar la funcionalidad inalámbrica de su marcapasos después de haber estudiado las posibilidades de que el dispositivo fuera accedido subrepticiamente para tomar control de él y quizás causarle la muerte.[56]

Barnaby Jack, el experto en seguridad que probó la posibilidad de que ese tipo de ataque ocurriera, había logrado también en otra ocasión que un cajero automático expulsara billetes de manera ininterrumpida. Igualmente, había *hackeado* una bomba de insulina para que hiciera una descarga letal del medicamento.[57] “Si se puede acceder remotamente al dispositivo siempre habrá posibilidades de abusar de él”, dijo en una entrevista.[58]

Otro ejemplo interesante se dio en 2010, cuando se descubrió un virus informático –llamado Stuxnet– que por cerca de dos años había pasado inadvertido para las empresas de seguridad. Este se propagaba a través de memorias externas USB y tenía el objetivo de infectar las computadoras que controlaban ciertas centrifugadoras utilizadas en el proceso de enriquecimiento de uranio. Como la mayoría de ataques parecían ocurrir en una planta nuclear cerca a la

---

55 *Véase,* Roman, Rodrigo, Zhou, Jianying, López, Javier, “*On the features and challenges of security and privacy in distributed internet of things*”, en: *Computer Networks*, Vol. 57, N. 10, 2013.

56 V*éase, “Yes, terrorists could have hacked Dick Cheney's heart*”, en: The Washington Post, 21 de octubre de 2013, disponible en: http://wapo.st/20EpPEd, consultado el 30 de noviembre de 2014.

57 *Véase,* CSOM, “*Lethal medical device hack taken to next level*”, disponible en: http://bit.ly/1R-Yimya, última consulta: 30 de noviembre de 2014.

58 *Véase,* Alexander, William, “*Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode*”, en: *Vice*, disponible en: http://bit.ly/1UGCpiE, última consulta: 30 de noviembre de 2014.

ciudad de Natanz, en Irán, se entendió que el propósito del virus era sabotear el programa de energía nuclear de este país.[59] El caso no solo quedó como antecedente de la guerra digital entre potencias; un virus con tal capacidad de camuflaje y expansión podría fácilmente tomar control de redes completas de objetos y dispositivos. Este tipo de virus está apenas emergiendo. Recientemente se descubrió Regin, tan complejo y sofisticado como Stuxnet, aunque orientado al robo de datos y espionaje. Aún es materia de investigación.[60]

En conclusión, cualquier cosa conectada a la red puede ser accedida clandestinamente y obligada a actuar de forma impredecible y dañina. Por supuesto, las consecuencias y dimensiones del daño que provoque la manipulación de cada dispositivo dependerán de sus funciones. Por eso, Adam Greenfield propone que los "sistemas ubicuos tengan por defecto un modo de configuración que asegure la seguridad física, psíquica y financiera del usuario".[61] Enunciada en teoría, la idea parece sensata, pero su aplicación práctica es a todas luces un reto aparte.

V. Conclusiones

Buena parte de la bibliografía que encontramos sobre internet de las cosas está relacionada con su futuro, sus posibilidades y el valor en el mercado de uno u otro servicio.[62] Y, como se planteó a lo largo de este documento, no se trata de un área de estudio en tecnología o ingeniería, sino de una sumatoria de cosas con el antecedente común de la computación ubicua y un presente ineludiblemente atado a internet. Esto abre de entrada un camino de trabajo para quienes quieran ahondar en el tema. Partiendo de ese supuesto central, hacemos las siguientes conclusiones y recomendaciones:

---

[59] Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown Publishing Group, 2014.

[60] *Véase,* Marquis-Boire, Morgan, Guarnieri, Claudio, y Gallagher, Ryna, "*Secret malware in European Union attack linked to U.S. and british intelligenc*", en: *The Intercept*, 24 de noviembre de 2014, disponible en: http://bit.ly/1P3ou4v, última consulta: 30 de noviembre de 2014.

[61] Greenfield, Adam, *supra* nota 10, p. 500. Traducción propia.

[62] *Véanse*, Kellmereit, Daniel, Obodovski, Daniel, *supra* nota 18; Gartner, "*Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business*", agosto de 2014, disponible en: http://gtnr.it/1swZR7r, última consulta: 30 de noviembre de 2014.; Press, Gill, "*Internet of Things By The Numbers: Market Estimates And Forecasts*", en: Forbes, 22 de agosto de 2014, disponible en: http://onforb.es/1KnOXef, última consulta: 30 de noviembre de 2014; Greenough, John, "*The 'Internet of Things' Will Be The World's Most Massive Device Market And Save Companies Billions Of Dollars",* en: *Business Insider*, noviembre de 2014. Disponible en http://read.bi/1v6KDqQ, última consulta: 30 de noviembre de 2014.

- Los riesgos en materia de privacidad, seguridad y autonomía que surgen en la IoT no son distintos a los que encontramos asociados hoy al entorno digital en general. Si hubiera que plantear alguna diferencia, ésta reside en la escala: en un contexto de IoT, estos riesgos parecen acentuarse.
- Entre todos los problemas identificados, el de privacidad –en el sentido planteado en este documento– parece el más grave. Pensada desde el diseño y la ingeniería –y con una veta claramente comercial– la IoT no incorpora un análisis sobre este punto, a pesar de que la “privacidad por diseño” o, dicho de otra forma, la inclusión de la privacidad en las arquitecturas y los dispositivos, no es un tema nuevo en el debate sobre tecnología y regulación.
- En un contexto como el latinoamericano, donde los esquemas de identificación son generalizados, la idea de la IoT puede desembocar fácilmente en formas de discriminación y profundización de la brecha digital. Tal y como se presenta, los dispositivos y servicios asociados a la IoT harán parte de ofertas comerciales que solo un sector de la población podrá pagar.[63]
- Un escenario futuro de millones de dispositivos conectados a la red implicará una explosión exponencial del tráfico. Según el reporte anual de Cisco, en 2018 el 50% de todas las conexiones provendrán de un dispositivo móvil. Además, se multiplicarán 11 veces las conexiones existentes entre máquinas.[64] Es decir, darán cuenta de un 3% del tráfico en internet. Si esta realidad es desafiante para Estados Unidos o Europa, es abrumadora para los países de la región. Así, cualquier discusión sobre IoT debe tener en cuenta los retos que aún subsisten en infraestructura y acceso a internet.
- La decisión sobre estándares técnicos para conectar objetos a la red está relacionada con la gobernanza de internet. En particular, con la gestión de los recursos críticos. En consecuencia, resulta relevante que en esos escenarios se haga seguimiento al proyecto de la IoT, aterrizado en su real dimensión, como lo propone este documento.
- Donde la sociedad está organizada alrededor de la tecnología, el poder tecnológico es la principal forma de poder.[65] Un entorno digital

---

[63] *Véase,* Bohn, Jürgen, *supra* nota 29.

[64] *Véase,* Cisco, “*Cisco Virtual Network Index”,* disponible en: http://bit.ly/1JVF8Eu, última consulta: 30 de noviembre de 2014.

[65] *Véase,* Feenberg, Amdrew, *Between Reason and Experience: Essays in Technology and*

conectado y omnipresente va más allá de los servicios y funciones que ofrece. La configuración de una arquitectura es el resultado de configuraciones de poder que a su vez lo distribuyen y reproducen. Esto implica aproximarse críticamente al proyecto comercial del IoT, sin desconocer sus virtudes y sin desestimar sus problemas.

- Para la sociedad civil resulta fundamental abrir espacios de interlocución para participar en este tipo de discusiones. Desde la perspectiva de la industria, es difícil tomar en cuenta posibles externalidades, en términos de derechos fundamentales, que traigan tecnologías omnipresentes. En cambio, las organizaciones, centros de pensamiento, universidades y grupos ciudadanos, pueden ofrecer una perspectiva distinta.

Modernity, Cambrige, MIT Press, 2010, p. 80.

La regulación de la pornografía no consentida en Argentina [1]

Paula Vargas de Brea[2]

Resumen

El objeto de esta investigación es proveer al regulador o al juez de una descripción del derecho vigente que les permita aplicarlo o resolver, en su caso, si hace falta otro tipo de regulación que brinde soluciones efectivas y respetuosas de todos los derechos humanos.

La pornografía no consentida es un problema global que merece atención regulatoria. Cualquier iniciativa de regulación debe partir de una definición clara del problema que se pretende regular. El presente capítulo ofrece elementos para llegar a una definición de pornografía no consentida y su comparaciones con figuras similares. Luego, desde un abordaje desde la perspectiva de los derechos humanos, se analizan las tensiones con el derecho a la libertad de expresión y las consecuencias de calificar a la pornografía no consentida como discurso no protegido. Por último, se analizan argumentos para su criminalización, que debe ser siempre la última ratio regulatoria.

1 Esta investigación contó con el invalorable aporte de las jornadas y talleres realizados en el Centro de Estudios para la Libertad de Expresión (CELE), durante los cuales tanto los investigadores del CELE, como su director e investigadores de otras disciplinas contribuyeron a evaluar y desarrollar muchos de los conceptos plasmados aquí.

2 Esta investigación fue realizada por Paula Vargas de Brea, investigadora del Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo, para proyectos de la Iniciativa Libertad de Expresión e Internet. Es abogada, coordinadora del Programa de Derecho de Internet y Tecnología de las Comunicaciones de la Universidad de San Andrés y profesora de la Facultad de Derecho de la Universidad de Buenos Aires.

I. Introducción

Las conductas y la relaciones humanas que el derecho pretende regular se modifican con el tiempo y con el contexto. El entorno tecnológico y digital en el que la sociedad (o la mayor parte de ella) vive en la actualidad ha introducido cambios radicales, que no se limitan solo a la forma en que nos comunicamos sino al contenido de lo que se comunica. Internet, unida a la banda ancha móvil, a la digitalización y a las tecnologías móviles permite a los individuos comunicar contenidos con un nivel de inmediatez, masividad, personalización y claridad como no lo permitía ninguna tecnología de la era analógica, ni siquiera consideradas en conjunto.

Estas condiciones han permitido el florecimiento de nuevas relaciones sociales, en general identificadas con el prefijo "ciber": ciberusuarios, ciberamigos, ciberterroristas, etc., y, entre ellas, las cibervíctimas.

La categoría de víctima y victimario se redimensiona frente a internet. Esta clasificación, tan antigua como las sociedades mismas, adopta ahora las características propias de internet. El ataque será personalizado y, al mismo tiempo, potencialmente masivo. Masivo en cuanto a su difusión pero también en cuanto a los participantes del mismo.

Algunos de los ataques de los cibervictimarios reproducen conductas que pueden realizarse en el mundo físico, solo que en línea se llevan a cabo con mucha mayor facilidad (por ejemplo, el robo de identidad). Pero otras, adquieren modalidades únicas y, por lo tanto, colocan a la víctima y a la sociedad en una situación de mayor indefensión y conmoción, ya que son imprevisibles y difíciles de conjurar.

Este es el caso de lo que mayoritariamente se ha llamado en la doctrina como "pornografía de venganza", término bajo el cual quedan incluidos distintos supuestos que giran básicamente en torno a la publicación no consentida, en internet o utilizando comunicaciones electrónicas, de imágenes sexuales. Esta definición básica se amplía o se restringe según el enfoque y el objetivo regulatorio. Como se explica luego, adoptaremos para el análisis regulatorio de esta investigación el término "pornografía no consentida".

Ejemplos de esta situación abundan cada vez más en todo el mundo[3] y su notoriedad e impacto ha sido reconocida por los reguladores, el sector privado prestador de servicios de internet, la sociedad civil y la academia.

---

[3] Por ejemplo, en México la policía cibernética del Distrito Federal registró 752 delitos de este tipo en el año 2014. *Véase*, Ochoa, Stephanie, "Venganzas amorosas con pornografía en internet", en: Milenio, 11 de enero de 2015, disponible en: http://bit.ly/1VHjhRG.

Como refiere Mary Anne Franks, quien ha elaborado una Guía para Reguladores:

> Tantos como 3 000 sitios web publican “pornografía de venganza” y ese material íntimo es asimismo ampliamente distribuido sin consentimiento a través de redes sociales, blogs, correos electrónicos y mensajes de texto. La Cyber Civil Rights Initiative (CCRI) es contactada por un promedio de 20-30 víctimas cada mes. La tecnología y las redes sociales han permitido a los abusadores externalizar distribuidamente (*crowd-source*) su acoso y también ha permitido a los individuos inescrupulosos aprovecharse de ello.[4]

El informe de la Association for Progressive Communications (APC) de 2015 ha caracterizado a la violencia contra las mujeres ejercida utilizando tecnología (VAW, por su nombre en inglés) como un *continuum*:

> La VAW no está fragmentada; es un *continuum*. La VAW relacionada con la tecnología está presente en este *continuum* tanto como en la VAW fuera de línea, donde ambas son experiencias conectadas y generadas por las relaciones inequitativas de poder enraizadas en la sociedad. Las mismas formas de discriminación por género que modelan las estructuras sociales, económicas, culturales y políticas se reproducen en línea y en las diferentes plataformas digitales. Contrariamente a las creencias populares, la VAW relacionada con las tecnología no es esporádica sino que es un evento que ocurre a diario en las vidas y experiencias de las mujeres y niñas alrededor del mundo.[5]

De acuerdo a lo que manifiestan algunas organizaciones y académicos, este tipo de acciones afectan en su amplia mayoría a las mujeres y ello es porque su desvalorización por el hecho de ser mujeres incluye la exposición de sus preferencias y actitudes sexuales. Es un claro exponente de la reproducción de patrones culturales discriminatorios. Al varón la exposición de su actividad sexual en general no lo desprestigia socialmente, mientras que a la mujer sí.

No debe soslayarse que la pornografía no consentida, al representar una situación sexual, expone a la víctima un tipo particular de violencia, que es la violencia sexual, aún cuando sea de tipo psicológico y no físico.

---

4 Franks, Mary Anne, *Drafting an Effective “Revenge Porn” Law: A Guide to Policymakers en End Revenge Porn,* disponible en: http://bit.ly/23H7kRZ. Traducción propia.

5 Women’s Legal and Human Rights Bureau, Inc., Association for Progressive Communications (APC), *End violence: Women's rights and safety online From impunity to justice: Domestic legal remedies for cases of technology-related violence against women,* APC, 2015, disponible en: http://bit.ly/1nDnniA.

Los casos reportados son todos dramáticos para las víctimas, algunas de las cuales llegaron a cometer suicidio o experimentaron graves daños psicológicos y vieron su vida familiar y laboral arruinada.[6] Efectivamente, esta conducta, perpetrada en general por varones en contra de mujeres, provoca grandes sufrimientos en las víctimas por la exposición de su intimidad ante la sociedad y, además, perjuicios materiales generados por las dificultades laborales que les acarrea la publicación o la disponibilidad de dicho material. En casos extremos ha implicado la necesidad de mudarse, de cambiar de trabajo y a sus hijos de escuela.

Por ejemplo, Chrissy Chambers –una "estrella" de la plataforma Youtube– inició un juicio civil en Inglaterra en procura de obtener daños y perjuicios contra su ex pareja, un británico que habría publicado material de contenido sexual, explícito, luego de su ruptura. Chambers expresó: "La primera vez que vi los videos, sentí que me habían arrebatado mi dignidad. Fue como recibir un golpe en el pecho que no me permitía respirar".[7] Esta declaración da una noción bastante clara de las consecuencias espirituales y físicas que experimentan las víctimas.

En Estados Unidos, el puntapié inicial para el proceso regulatorio de la pornografía de venganza fue el caso de Holly Jacobs[8], quien hasta debió cambiar legalmente su nombre (su nombre de nacimiento es Holli Tometz) por el acoso que sufrió luego de que su ex pareja hiciera públicas imágenes intimas sin su consentimiento. Sus planes personales y profesionales se truncaron y debió dedicar tiempo y esfuerzo a tratar de contener el daño creado por la propagación de dichas imágenes. Finalmente creó *End Revenge Porn*[9], una campaña organizada por la Cyber Civil Rights Initiative para promover la sanción de legislación y ayudar a otras víctimas.

En honor a la brevedad no se brindarán ejemplos de otros casos, pero la mayoría han sido acabadamente documentados por Danielle Citron, referente académica en el tema y activista, en su libro *Delitos de odio en el ciberespacio.*[10]

El problema no está visibilizado en la Argentina ya que no existen estadísticas oficiales[11] que hayan estudiado de forma desagregada el fenómeno de

---

6 *Ibíd.*, p. 14.

7 Press Association, "*YouTube star in revenge porn case*", en: *The Press*, 3 de junio de 2015, disponible en: http://m.yorkpress.co.uk/news/13310632.YouTube_star_in__revenge_porn__case/

8 *Véase,* Jacobs, Holly, "*Victims of Revenge Porn deserves real protection*", en: *The Guardian*, 8 de octubre de 2013, disponible en: http://bit.ly/23H7tEU.

9 *Véase,* http://www.endrevengeporn.org/.

10 Citron, Danielle Keats, *Hates Crimes in Cyberspace*, Harvard University Press, 2014.

11 No han publicado estadísticas sobre este fenómeno ni el Observatorio de la Violencia contra

la pornografía no consentida, por lo cual no está claro en qué grado ocurre. Dada la masividad en el uso de dispositivos tecnológicos para la comunicación, puede presumirse que la falta de visualización se debe más a un defecto en la forma en que se recolectan los datos estadísticos que a la inexistencia del problema.

No obstante su invisibilización en el campo estadístico, la pornografía no consentida es de interés regulatorio ya que existe claramente un derecho vulnerado y en nuestro sistema jurídico, si existe un derecho vulnerado debe preverse un mecanismo para su reparación. Por lo tanto, la cuestión no es si debe regularse sino cómo.

En general, el objetivo de la víctima de una situación de pornografía no consentida es: a) obtener la remoción inmediata del contenido; b) sancionar penalmente al agresor; y c) obtener una reparación económica por los perjuicios sufridos.

El regulador o los jueces pueden, a través del derecho, satisfacer todas o algunas de estas pretensiones. No obstante, antes de adoptar una solución regulatoria o de interpretar el derecho vigente, deberán hacer un balance con otros derechos, principalmente con el derecho a la libertad de expresión y el acceso a la información, ya que la pornografía no consentida implica circulación de contenido.

Es decir, uno de los puntos más relevantes a considerar en relación con la pornografía no consentida es que la conducta se refiere a la publicación o puesta a disposición de contenido, por lo cual, debe incluir un análisis sobre la legitimidad para limitar la libertad de expresión, sea porque se criminaliza a quien se expresa y/o se le imponen sanciones pecuniarias y/o se prohíbe la circulación de este contenido. En consecuencia, cada opción regulatoria debe ser confrontada con el mecanismo dispuesto en el artículo 13 de la Convención Americana de Derechos Humanos, en particular a la luz de la restricción de contenidos en internet, que tiene su doctrina específica.

Ya en el año 1995, cuando Naciones Unidas, en la Cuarta Conferencia Mundial de Mujeres estableció la Plataforma de Beijing, se tuvo en cuenta que el abordaje de la relación entre los medios, la cosificación de las mujeres y la violencia de género debían considerar los límites que el derecho a la libertad

las Mujeres del Consejo Nacional de las Mujeres, ni el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI), ni la Oficina de Violencia Doméstica de la Corte Suprema de Justicia de la Nación, ni la Unidad Fiscal Especializada de Violencia contra las Mujeres, entre otros organismos con competencia para relevar la pornografía no consentida.

de expresión imponen.[12] Allí se dispuso como uno de los objetivos a lograr por los gobiernos y las organizaciones internacionales "dentro de lo consistente con la libertad de expresión (…) adoptar medidas efectivas o establecer dichas medidas, incluyendo la legislación apropiada contra la pornografía y la proyección de la violencia contra las mujeres y los niños en los medios".[13]

El objeto de esta investigación es proveer al regulador o al juez de una descripción del derecho vigente que les permita aplicarlo o resolver, en su caso, si hace falta otro tipo de regulación que brinde soluciones efectivas y respetuosas de todos los derechos humanos.

En principio, se desarrollarán dos perspectivas desde las cuales puede ser abordada esta cuestión, que no son excluyentes entre sí:

a) Como la vulneración de un derecho fundamental. Desde esta perspectiva se analizará si la pornografía no consentida constituye un supuesto de discurso de odio por incitar a la violencia contra las mujeres o si es un contenido que vulnera la privacidad de la víctima. También podría constituir un supuesto de violación a la ley de protección de datos personales, pero no será objeto de tratamiento en este trabajo ya que bajo el Sistema Interamericano no está claro que sea un derecho fundamental independiente de la privacidad, no obstante lo cual, la acción de hábeas data puede ser un recurso procesal eficiente.

b) Como un acto que requiere condena penal. Se analizará si la pornografía no consentida está contemplada en algún tipo penal ya existente y, en su caso, si es recomendable su criminalización.

Por otra parte, se analizará cuáles son los remedios que el Código Civil y Comercial puede aportar para la reparación de los eventuales daños y cuál sería la vía procesal más adecuada.

II. Definición de pornografía no consentida y comparación con otras figuras similares

Elegimos delimitar el objeto de esta investigación a lo que denominamos pornografía no consentida, definida como la publicación o puesta a disposición –o la amenaza de hacerlo– al público en general o de terceros en particular, de forma deliberada, utilizando la internet u otra tecnología de la comunicación

---

12 Organización de Naciones Unidas, Plataforma de Beijing, 1995, disponible en: http://bit.ly/1hj4YFs.

13 *Ibíd.*

de imagen/es, o audio/s o contenido/s audiovisual/es de naturaleza sexual explícita, sin el consentimiento de la víctima, por parte de un individuo con el que ésta hubiera mantenido una relación íntima.

Consideramos que esta es la definición que permite mantener un equilibrio entre los derechos que pueden estar en pugna con el derecho de la víctima, como lo es la libertad de expresión.

Esta definición se diferencia de otras situaciones que regulan fenómenos parecidos como por ejemplo:

- *Acoso (o ciberacoso):* esta es una figura que integra pero a la vez excede al supuesto de pornografía no consentida. El ciberacoso y el ciberacecho han sido definidos por Danielle Citron como:

> (…) la conducta que implica la intención de generar un daño emocional substancial infligido a través del uso de internet, de manera tal que constituye un curso de acción más que un hecho aislado. El ciberacecho tiene en general un significado más acotado: es una conducta en internet que provoca a un individuo temor por su vida o seguridad o que podría provocar a un individuo razonable temor por su vida o su seguridad”.[14]

Estas conductas requieren para su configuración una situación sostenida en el tiempo, conformada por varias conductas de las cuales la pornografía no consentida es una de ellas. Implica además la intención de dañar a la víctima. Citron aclara que el prefijo “ciber” es válido por cuanto reafirma el incremento de los efectos negativos de la conducta que ocurren solo en internet.

- *Pornografía de venganza*[15]: ha sido definida, también por Citron[16,] como “la publicación de fotografías de desnudos sin consentimiento. Es una demostración de que el ciberacoso es una cuestión de género”. A los fines de esta investigación, se ha optado por una definición que prescinda de la intencionalidad “de venganza”. En nuestra definición, es suficiente que la acción cometida por un individuo con el que la

---

14 Citron, Danielle Keats, *supra* nota 10, posición 70 de 6510 en *ebook*. Traducción propia.

15 Cuando esta investigación se refiera al término “pornografía de venganza” y no a “pornografía no consentida”, que es nuestra propia definición del objeto de estudio, será porque la fuente originaria se refería a dicho término.

16 Citron, Danielle Keats, *supra* nota 10, posición 300 de 6510 en *ebook*. Traducción propia.

víctima mantenía una relación sentimental de confianza y que sea deliberada, es decir, que no sea producto de un error.

Por otra parte, se explica a continuación el porqué se han incluido determinados elementos y excluido otros:

- *Publicación o puesta a disposición por parte de alguien que tiene o tuvo una relación íntima con la víctima:* se excluye la publicación o posterior difusión por parte de terceras personas ajenas a una relación sentimental o relación de tipo sexual consentida con la víctima. Esta acción podrá eventualmente derivar en una acción civil por daños y perjuicios, o configurar algún otro delito. Pero, por razones de libertad de expresión y de intencionalidad, se excluye de las propuestas regulatorias de este estudio, aun cuando el material de la publicación o difusión hubiere sido puesto a disposición por el autor de la pornografía no consentida.

Más adelante se analizará, no obstante, la situación de las plataformas creadas específicamente para fomentar esta actividad, la extensión de la responsabilidad hacia otros sujetos como las plataformas en las que el material se publica o que prestan el servicio de conectividad o hacia quienes republican, con fines de lucro. Tampoco quedaría incluido el tercero que realiza la publicación o puesta a disposición por orden y voluntad de quien tuvo la relación íntima con la víctima.

En el concepto de "relación íntima" incluyen solo las relaciones de pareja. Se excluyen de este concepto las relaciones familiares, de amistad cercana o de empleo. Esto no quiere decir que aquel que publica o pone a disposición material íntimo de otra persona deba quedar eximido de toda responsabilidad, sino que deberá regularse bajo otra figura, aún cuando las consecuencias sean las mismas.

El objetivo de efectuar esta discriminación es poder controlar las consecuencias jurídicas en cada caso. La realización de dicha conducta por una ex o actual pareja puede tener una connotación de violencia de género que merece su análisis por separado. También podría tener una connotación de violencia de género la actitud de un empleador pero difícilmente pueda éste haber obtenido un material sexual a través de una relación de ese tipo. El elemento recurrente en las situaciones de pornografía no consentida es la relación de

confianza en el marco de la cual se produce el material íntimo. En el Reporte de Naciones Unidas *Un marco favorable a la acción para prevenir la violencia contra las mujeres* se hace referencia a "violencia de pareja íntima".[17]

De todas maneras, dentro de la definición podrían incluirse a las relaciones circunstanciales o a las situaciones sexuales grupales, de las que participara más de una persona (por ejemplo, quien toma las imágenes de otras personas en un acto sexual).

- *Incluye sólo imágenes, audios o material audiovisual de carácter sexual*: se excluye de esta investigación todo aquel material que si bien puede revelar la intimidad de la víctima no detenta un carácter sexual. No obstante, se incluyen las imágenes de desnudos aún cuando representen actos sexuales explícitos. También se incluyen audios porque la voz ha sido incluida en el nuevo Código Civil y Comercial como parte del derecho a la imagen.
- *Es irrelevante si el material fue obtenido con consentimiento*: el foco de la investigación está colocado en los resultados de la acción y en la falta de consentimiento para la publicación o puesta a disposición, independientemente de que el infractor haya obtenido las imágenes de forma legítima. La falta de consentimiento en la obtención del material podrá eventualmente configurar otro delito o ilícito. La irrelevancia del consentimiento también impide que se realice un juzgamiento moral sobre la víctima por haber consentido la producción de un material de contenido sexual.[18]

---

17 *Véase,* UN Women, *A Framework to underpin action to prevent violence against women,* 2015, p. 10, disponible en: http://bit.ly/1Nlz4Qv.

18 *Véase,* Corte Constitucional de Colombia, sentencia 634-13, disponible en: http://bit.ly/1O-yMApE: "La juez de primera instancia asumió que la accionante creó el riesgo y que por ello debía asumir la responsabilidad sobre los efectos de la publicación de las imágenes. El uso descalificativo o basado en estereotipos de la palabra "permisiva" en el contexto referido, además, degrada a la accionante y a las mujeres en general en un sentido doble. De un lado, la juez de instancia realiza una transferencia de responsabilidad a la accionante de todos los efectos relacionados con la autorización otorgada, como resultado de la descalificación del comportamiento de la accionante a partir de un estereotipo del comportamiento esperado de ella construido sobre la base del prejuicio según el cual el tipo de fotos que le tomaron tenían un contenido al menos reprochable. De otro lado, el uso de la palabra 'permisiva' en el contexto presentado, indirectamente juzga el comportamiento de otras mujeres que en desarrollo de su libertad no solo deciden libremente tomarse fotos como las que se aportaron al presente proceso sino que aprueban su publicación y circulación. Estos usos del lenguaje resultan contrarios a la garantías constitucionales de no discriminación y deben, por lo tanto, prevenirse."

- *Incluye sólo relaciones entre adultos:* en una relación entre menores o entre un menor y un adulto, por defecto no puede existir consentimiento para la relación sexual en sí. La publicación de este tipo de material configuraría un supuesto de pornografía infantil.
- *No se requiere la producción de un daño:* el daño debe presumirse en estos casos. No se trata de que no sea un elemento del supuesto regulado, se trata de que no deba probarse por parte de la víctima puesto que la mera prueba podría colocarla en situaciones humillantes. Tampoco es elemento necesario de la definición brindada en esta investigación que se ponga en peligro la vida o la integridad física de la víctima.
- *Se excluye la publicación o puesta a disposición que ocurre en otros ámbitos ajenos a internet o a las comunicaciones electrónicas:* el objeto de la presente investigación se refiere a la publicación o puesta a disposición que ocurre utilizando internet o a través de alguna otra tecnología de las comunicaciones como telefonía móvil, correos electrónicos, etc.

No obstante, hacemos notar que Mary Anne Frank[19] recomienda no limitar la definición al ámbito de internet o las comunicaciones sino que propone ampliarla a todo tipo de tecnología, como los DVD, por ejemplo.

- *No se requiere una intencionalidad en particular por parte del autor:* si bien se requiere voluntariedad, lo cual excluye el error, no es necesario que el autor tenga una intención en particular. Basta con que conozca que no está autorizado para publicar o poner a disposición ese material.
- *Es irrelevante si el material se refiere a una relación entre la víctima y el autor de la publicación o entre la víctima y otra persona o si la víctima es reconocible o no:* este es un punto importante. El material debe publicar imágenes, audios o contenidos audiovisuales de la víctima, sin importar si se refieren a la relación mantenida con el autor/agresor o con otra persona, si son actuales o antiguas. Tampoco consideramos importante que la víctima pueda ser reconocida o no, ya que lo importante es que la propia víctima sepa que es material relacionado con su persona.
- *Incluye las amenazas:* es importante incluir la amenaza cierta de publicar o poner a disposición el material porque esta acción ya implica violencia o vulnera la privacidad, al limitar la libertad de acción de la víctima y crearle una situación de angustia.

---

19 *Véase,* Franks, Mary Anne, *supra* nota 4.

III. La Pornografía no consentida desde la perspectiva de los Sistemas de Derechos Humanos

Las distintas convenciones y documentos que integran los Sistemas de Derechos Humanos de Naciones Unidas y de la Organización de los Estados Americanos, imponen obligaciones y estándares de protección de los individuos a ser cumplidos por los Estados en la actuación de sus distintos organismos.

Partiendo de la definición de pornografía no consentida adoptada en el presente documento, dos derechos especialmente regulados por los Sistemas de Derechos Humanos aparecen como adecuados para regular esta conducta: el derecho de las mujeres a no ser víctimas de violencia de género, lo que autorizaría a calificar a la pornografía no consentida como una especie de "discurso de odio"; y el derecho de los individuos a la privacidad.

Desde ya se adelanta que la calificación de la pornografía no consentida como un caso de discurso de odio permitiría acciones legales de remoción de contenido más eficaces que su calificación como un caso de discriminación (no por género) o de violación de la privacidad.

1. La pornografía no consentida como un supuesto de discurso de odio por incitar a la violencia contra la mujer[20]

Se analizará a continuación el supuesto de pornografía no consentida en relación con los estándares de la violencia de género, y su potencial regulación como discurso de odio en el marco del derecho a la libertad de expresión del Sistema Interamericano. Como se dijo anteriormente, la conducta ejercida en los casos de pornografía no consentida se refiere a la circulación de contenido y su penalización podría implicar la restricción de dicha circulación, cuya legitimidad depende del cumplimiento de los estándares de protección de la libertad de expresión.

---

[20] Este estudio hará referencia sólo al Sistema Interamericano. Si bien no existe mucha jurisprudencia de la Corte Interamericana de Derechos Humanos en materia de discurso de odio, la misma ha dicho en la Opinión Consultiva OC-5/85, La Colegiación Obligatoria de Periodistas (artículos 13 y 29 de la Convención americana sobre Derechos Humanos), 13 de noviembre de 1985, Ser. A N. 5, párr. 51, que: "En verdad, frecuentemente es útil comparar la Convención Americana con lo dispuesto en otros instrumentos internacionales como medio para poner de relieve aspectos particulares de la regulación de un determinado derecho, pero tal método no podría emplearse nunca para incorporar a la Convención criterios restrictivos que no se desprendan directamente de su texto, por más que estén presentes en cualquier otro tratado internacional."

1.1. La violencia de género como una forma de discriminación

La pornografía no consentida y sus otras variantes como el ciberacoso y la pornografía de venganza han sido abordadas como un problema de género en todas las jurisdicciones en las que ha sido regulada.[21] De acuerdo a las estadísticas disponibles, la pornografía no consentida es una problemática que afecta más a mujeres que varones[22] lo que se explica fácilmente por su connotación sexual. Como se describirá a continuación, la utilización del sexo como un método de privación de la dignidad es típica de los parámetros machistas de violencia y discriminación.

Las violaciones de mujeres en las guerras como arma para humillar al enemigo; el forzamiento a exponer la desnudez a las mujeres encarceladas; y los altos índices de feminicidios en lugares tradicionalmente muy machistas; todos casos que fueron considerados por la jurisprudencia de la Corte IDH –se citan más abajo– representan situaciones equivalentes a la pornografía no consentida, tanto por el contexto en que ocurren como por la desproporción con la que le ocurre a las mujeres.

La violencia contra las mujeres y la discriminación contra las mujeres están reguladas por los mismos instrumentos internacionales. La Convención de Belém do Pará[23] y la Convención sobre la eliminación de toda forma de discriminación contra la mujer (CEDAW, por sus siglas en inglés)[24] –en particular la Recomendación 19[25]–, han vinculado la violencia contra las mujeres y la discriminación, y han considerado a la violencia como una especie de discriminación. También el Convenio del Consejo de Europa sobre Prevención y Lucha contra la Violencia contra las Mujeres y la Violencia Doméstica (Estambul, 2011) afirma que: "(…) la violencia contra las mujeres es una manifestación de desequilibrio histórico entre la mujer y el hombre que ha llevado a la dominación y a la discriminación de la mujer por el hombre, privando así a la mujer de su plena emancipación", y que "la naturaleza estructural de

---

21 *Véase,* USA Hispanic, *Australia proposes to criminally punish "revenge porn",* 12 de octubre de 2015, disponible en: http://bit.ly/1QF1eKK.

22 "Dos tercios de los incidentes involucraron a mujeres de menos de 30 años de edad, siendo los sospechosos mayoritariamente sus ex parejas. Por cada ocho reclamos iniciados por mujeres se hizo 1 reclamo de un hombre". Traducción propia. *Véase,* Davis, Caroline, *Revenge Porn cases increase considerable, pólice figures reveal*, en. The Guardian, 16 de Julio de 2014, disponible en: http://bit.ly/1K8UdS4.

23 Organización de los Estados Americanos, *Convención de Belem do Pará,* 1994, disponible en: http://bit.ly/1cJ5i72.

24 Organización de Naciones Unidas, *Convención sobre la eliminación de toda forma de discriminación contra la mujer*, 1979, disponible en: http://bit.ly/VJkZJY.

25 *Ibíd.*, recomendación 19.

la violencia contra las mujeres está basada en el género".[26] La CEDAW define la discriminación contra la mujer como:

> (…) toda distinción, exclusión o restricción basada en el sexo que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio por la mujer, independientemente de su estado civil, sobre la base de la igualdad del hombre y la mujer, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera.[27]

En el ámbito interamericano, la Convención Belém do Pará señala que la violencia contra la mujer es "una manifestación de las relaciones de poder históricamente desiguales entre mujeres y hombres" y reconoce que el derecho de toda mujer a una vida libre de violencia incluye el derecho a ser libre de toda forma de discriminación. La CEDAW ha declarado que la definición de la discriminación contra la mujer "incluye la violencia basada en el sexo, es decir, la violencia dirigida contra la mujer (i) porque es mujer o (ii) que la afecta en forma desproporcionada". La CEDAW también ha señalado que "[l] a violencia contra la mujer es una forma de discriminación que impide gravemente que goce de derechos y libertades en pie de igualdad con el hombre".[28]

En Argentina, la ley 26 485 de Protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales entiende por violencia contra las mujeres:

> (…) toda conducta, acción u omisión, que de manera directa o indirecta, tanto en el ámbito público como en el privado, basada en una relación desigual de poder, afecte su vida, libertad, dignidad, integridad física, psicológica, sexual, económica o patrimonial, como así también su seguridad personal. Quedan comprendidas las perpetradas desde el Estado o por sus agentes. Se considera violencia indirecta, a los efectos de la presente ley, toda conducta, acción u omisión, disposición, criterio o práctica discriminatoria que ponga a la mujer en desventaja con respecto al varón.[29]

---

26 Consejo de Europa, *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica,* Estambul, 2011, disponible en: http://bit.ly/1SVYonY.

27 Organización de Naciones Unidas, *supra* nota 24, antecedente 3.

28 Organización de Naciones Unidas, *supra* nota 25, párrs. 1 y 6.

29 Ley No. 26 485 de Protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales, B.O. 14/04/09, Art. 4

En particular, esta ley recepta a la "violencia mediática" como un tipo de violencia contra las mujeres.[30]

Todos estos instrumentos legales llaman al Estado a proteger a las mujeres contra la violencia, y la discriminación entendida como una forma de violencia, no solo de los actos del propio Estado sino también de los cometidos por las organizaciones, las empresas y cualquier otro privado.[31]

A nivel jurisprudencial, la Corte IDH ya ha interpretado, por ejemplo, en el caso Penal Miguel Castro Castro que existen patrones de conducta que afectan solo a las mujeres por ser consideradas inferiores y que esa discriminación es la causa de acciones violentas contra ellas. En dicho caso, la Corte IDH señaló que las mujeres detenidas o arrestadas "no deben sufrir discriminación, y deben ser protegidas de todas las formas de violencia o explotación".[32] Dicha discriminación incluye "la violencia dirigida contra la mujer porque es mujer o que la afecta en forma desproporcionada", y que abarca "actos que infligen daños o sufrimientos de índole física, mental o sexual, amenazas de cometer esos actos, coacción y otras formas de privación de la libertad".[33]

También la Corte Constitucional de Colombia se ha referido a la violencia ocurrida dentro del ámbito matrimonial, o de pareja, como violencia de género y la ha encuadrado dentro del artículo 12 de la Constitución, según el cual "nadie será sometido a desaparición forzada, a torturas ni a tratos o penas crueles, inhumanos o degradantes"[34] (en algunos fallos de la Corte IDH la violación sexual también es asimilada a la tortura). En ocasión de la aprobación de la Convención de Belem do Pará dijo la Corte Constitucional que:

> Las mujeres están sometidas a una violencia, si se quiere, más silenciosa y oculta, pero no por ello menos grave: las agresiones en el ámbito doméstico y en las relaciones de pareja, las cuales son no sólo *formas prohibidas de*

30 *Véase, Ibíd.*, Art. 6: "f) Violencia mediática contra las mujeres: aquella publicación o difusión de mensajes e imágenes estereotipados a través de cualquier medio masivo de comunicación, que de manera directa o indirecta promueva la explotación de mujeres o sus imágenes, injurie, difame, discrimine, deshonre, humille o atente contra la dignidad de las mujeres, como así también la utilización de mujeres, adolescentes y niñas en mensajes e imágenes pornográficas, legitimando la desigualdad de trato o construya patrones socioculturales reproductores de la desigualdad o generadores de violencia contra las mujeres."

31 *Véase,* Organización de Naciones Unidas, *supra* nota 25, párrafo 9.

32 Corte IDH, "Caso del Penal Miguel Castro Castro vs. Perú. Fondo, Reparaciones y Costas", sentencia del 25 de noviembre de 2006, Serie C, No. 160, párrafo 303.

33 *Ibíd.*

34 Corte Constitucional de Colombia, sentencia No. T-382/94, disponible en: http://bit.ly/1JVGsr2.

> *discriminación por razón del sexo* sino que pueden llegar a ser de tal intensidad y generar tal dolor y sufrimiento, que configuran verdaderas torturas o, al menos, tratos crueles, prohibidos por la Constitución y por el derecho internacional de los derechos humanos.[35]

Asimismo, la Corte IDH ha reconocido como casos de violencia sexual (aun cuando no esté tipificado como delito contra la integridad sexual), la violencia psicológica en un contexto en el que se utiliza el cuerpo o el sexo para privar a la víctima de su dignidad.

> El haber forzado a las internas a permanecer desnudas en el hospital, vigiladas por hombres armados, en el estado precario de salud en que se encontraban, constituyó violencia sexual en los términos antes descritos, que les produjo constante temor ante la posibilidad de que dicha violencia se extremara aún más por parte de los agentes de seguridad, todo lo cual les ocasionó grave sufrimiento psicológico y moral.[36]

> (…) la violencia sexual se configura con acciones de naturaleza sexual que se cometen contra una persona sin su consentimiento, que además de comprender la invasión física del cuerpo humano, pueden incluir actos que no involucren penetración o incluso contacto físico alguno. En particular, la violación sexual constituye una forma paradigmática de violencia contra las mujeres cuyas consecuencias, incluso, trascienden a la persona de la víctima.[37]

Podría trazarse un paralelismo entre la situación de violencia sexual física, ya abordada por la Corte IDH, y este tipo de violencia sexual psicológica que permiten ciertas tecnologías. Ambos tipos tienen como fuente la discriminación contra la mujer y como objetivo la destrucción de la dignidad y la estigmatización de la víctima en la sociedad en que se mueve. Si este no fuera el resultado esperado, la pornografía no consentida carecería de sentido para quien la comete.[38]

---

[35] Corte Constitucional de Colombia, sentencia C-408/96, disponible en: http://bit.ly/1TAeq6e. El resaltado es propio.

[36] *Ibíd.*, párrafo 11.

[37] Corte IDH, "Fernández Ortega y otros c/ México. Excepción Preliminar, Fondo, Reparaciones y Costas", sentencia del 30 de agosto de 2010, parr. 119.

[38] Corte IDH, *supra* nota 32: "La violación sexual de las mujeres fue una práctica del Estado, ejecutada en el contexto de las masacres, dirigida a destruir la dignidad de la mujer a nivel cultural, social, familiar e individual".

Paulatinamente, distintos documentos de organizaciones internacionales comenzaron a adoptar esta visión y a incorporar al mal uso de las tecnologías en el estudio de políticas contra la violencia de género.

Por ejemplo, en la 57º Reunión de la Comisión de la Condición de la Mujer (2013) se urgió a los gobiernos y a las partes interesadas relevantes (algunos actores del sector privado, por ejemplo) a:

> (…) desarrollar mecanismos para combatir el uso de las TIC y las redes sociales para perpetrar actos de violencia contra las mujeres y niñas, incluyendo el uso delictivo de las TIC para acoso sexual, explotación sexual, pornografía infantil y tráfico de mujeres y niñas y las formas emergentes de violencia como ciberacoso, ciber bullying, violaciones a la privacidad que ponen en riesgo la seguridad de mujeres y niñas.[39]

También en 2013, en la Asamblea General de Naciones Unidas se adoptó por consenso una resolución que dice:

> (…) las violaciones relacionadas con las tecnologías de la información, los abusos y la violencia contra las mujeres, incluyendo los defensores de los derechos humanos de las mujeres, tales como acoso en línea, ciberacecho, violaciones a la privacidad, censura y hackeo de correos electrónicos, teléfonos móviles y otros aparatos electrónicos, con el objetivo de desacreditarlas y/o incitar a otras violaciones y abusos contra ellas, son de creciente preocupación y la manifestación de la discriminación sistémica basada en el género, que requiere de respuestas efectivas compatibles con los derechos humanos.[40]

Asimismo, el reporte "Ciberviolencia contra mujeres y niñas: un llamado a la acción global", elaborado por la Comisión de Banda Ancha de Naciones Unidas para el desarrollo digital en 2015, convoca a interpretar la CEDAW "bajo el lente del siglo xxi".[41]

Más recientemente, la Directora Ejecutiva de ONU Mujeres mencionó a los "mensajes de texto abusivos" entre los casos de crímenes y abusos contra

---

[39] Organización de las Naciones Unidas, *57th Commission on the Status of Women,* 2013*,* disponible en: http://bit.ly/1X0vdiQ. Traducción propia.

[40] Organización de las Naciones Unidas, Resolución adoptada por la Asamblea General el 18 de diciembre de 2013, A/RES/68/181, disponible en: http://bit.ly/1kLtgEv.

[41] Broadband Comission for Digital Developement, *Cyberviolence against women and girls,* 2015, disponible en: http://bit.ly/1VgYyIz.

mujeres.[42]En el mismo sentido, por ejemplo, la legislación que prohíbe la pornografía de venganza en Israel considera a las víctimas como víctimas de delitos sexuales y a los victimarios como agresores sexuales.[43]Por su parte, el decreto reglamentario a la Ley 26 485 aclara que las definiciones de violencia contenidas en la ley no son restrictivas ni taxativas.[44]

En conclusión, la violencia contra las mujeres es la manifestación de la discriminación por género. En particular se considera a la violencia sexual, que incluye la violencia física (violaciones) y la psicológica ocurrida en contextos en los que el sexo es la excusa para humillar a la víctima.

2. La pornografía no consentida encuadra dentro de la violencia de género de tipo sexual

2.1. La violencia de género como un supuesto de discurso de odio

La pornografía no consentida es, como ya se dijo antes, contenido, expresión. Uno de los datos más relevantes que arroja el estudio de la pornografía no consentida es que logra una adhesión casi unánime a favor de su proscripción. Hasta los más acérrimos defensores de la libertad de expresión

---

42 "Imaginen lo diferente que sería el mundo para las niñas de hoy en día si pudiéramos evitar el matrimonio precoz y la mutilación genital femenina, la inacción frente a la violencia doméstica, los mensajes de texto abusivos, la impunidad de los violadores, la esclavización de las mujeres en las zonas en conflicto, el asesinato de defensoras y defensores de los derechos humanos de las mujeres o la hostilidad a la que se enfrentan las mujeres en las comisarías de policía o los tribunales cuando dan testimonio de la violencia sufrida." Declaración de la Directora Ejecutiva de ONU Mujeres, Phumzile Mlambo-Ngcuka, para el Día Internacional de la Eliminación de la Violencia contra la Mujer, 20 de noviembre de 2015, disponible en: http://www.unwomen.org/es/news/stories/2015/11/ed-message-intl-day-for-elimination-of-violence-against-women#sthash.apfc8fmF.dpuf.

43 "Estipula que aquellos encontrados culpables de la publicación de este tipo de contenidos serán enjuiciados como agresores sexuales, mientras que las víctimas serán reconocidas como víctimas de un delito sexual". Yaakov, Yifa, *"Israeli Law makes revenge porn a sex crime"* en: *The Times of Israel*, 6 de enero de 2014, disponible en: http://bit.ly/1PwWHen. Traducción propia.

44 Decreto No. 1011/2010, B.O. 20/07/2010, Art. 6: "Las definiciones de violencia comprendidas en el artículo que se reglamenta, en ningún caso pueden interpretarse en sentido restrictivo ni taxativo, como excluyentes de hechos considerados como violencia contra las mujeres por otras normas. Para ello deberá interpretarse la norma de forma armónica y sistemática con lo establecido en el artículo 4º, segundo párrafo de la Ley Nº 26 485, y con lo dispuesto en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer; la Convención sobre Eliminación de todas las Formas de Discriminación contra la Mujer; la Recomendación General Nº 19 del Comité para la Eliminación de la Discriminación contra la Mujer; los demás Tratados Internacionales de Derechos Humanos y las observaciones y recomendaciones que efectúen sus respectivos órganos de aplicación."

parecieran coincidir en que se trata de un tipo de discurso que no merece protección legal. Un supuesto similar al de la pornografía infantil.

Así, Neils Richards, autor del libro “Derechos civiles en la era digital” y defensor de la libertad de expresión, en un artículo escrito en coautoría con Danielle Citron (enérgica defensora de la regulación de la pornografía de venganza) dijo que:

> Muchos expertos legales –nosotros incluidos– hemos convocado a una mejor regulación de este problema importante y real. Esta convocatoria representaría un caso directamente dirigido a proteger a las personas de los peligros derivados de un rango entre el acoso y los delitos sexuales. No obstante, algunos críticos argumentan que regular la pornografía no consentida conlleva el riesgo de censurar discursos protegidos, incluyendo la pornografía. De acuerdo con la Primera Enmienda, dicen estos críticos, no podemos asumir ese riesgo. Pero es posible ser al mismo tiempo proponografía y antipornografía de venganza y las leyes pueden ser diseñadas a tal fin. Lo que importa, bajo la Primera Enmienda, y lo que muchas veces se malinterpreta, no es si puede o no regularse la pornografía de venganza sino cómo.[45]

La garantía de la libertad de expresión ha sido receptada en la Convención Americana de Derechos Humanos y en el artículo 14 de la Constitución Argentina, así como en todas las constituciones de América Latina. Lo que provoca esta garantía es la sospecha de inconstitucionalidad de cualquier restricción a este derecho.

Ahora bien, la proscripción de un contenido es posible, en el marco de la Convención Americana, si se trata de un caso de “discurso de odio”, único tipo de discurso directamente prohibido en el texto del artículo del 13, inciso 5, el cual dispone que:

> Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

---

45 Richards, Neils, Citron, Danielle, “*Regulate revenge porn isn't censorship: The disclosure of a nude photo in breach of trust and privacy is beneath the attention of the First Amendment*”, en: Aljazeera America, 1 de febrero de 2015, disponible en: http://bit.ly/1SCltKZ. Traducción propia.

Es notable que el sexo no haya sido explícitamente incluido dentro de los motivos mencionados como supuestos de apología del odio que incita a la violencia. No obstante, esto fue subsanado en el texto de la Convención de la CEDAW y en informes posteriores de la Relatoría Especial para la Libertad de Expresión (en adelante, RELE).

La jurisprudencia de la Corte Suprema de Justicia Argentina se ha referido al discurso de odio en pocos casos y no ha definido apología del odio o incitación a la violencia, pero los ha mencionado en algunos casos:

> Por ende, la interdicción de la discriminación en cualquiera de sus formas y la exigencia internacional de realizar por parte de los Estados acciones positivas tendientes a evitar dicha discriminación deben reflejarse en su legislación, de lo cual es un ejemplo la ley 23.592, y también en la interpretación que de tales leyes hagan los tribunales… De aquí se sigue que no se pueda legitimar como partido político a quienes incurren en apología del odio e, indirectamente, incitan a la violencia.[46]

La Corte Constitucional de Colombia, por su parte, ha dicho que:

> En criterio de la Corte, a la luz de las disposiciones constitucionales y de tratados internacionales sobre derechos humanos aplicables, estos tipos de expresión sobre los cuales se ha desvirtuado la presunción de cobertura constitucional de la libertad de expresión son cuatro: (a) la propaganda en favor de la guerra; *(b) la apología del odio nacional, racial, religioso o de otro tipo de odio que constituya incitación a la discriminación, la hostilidad, la violencia contra cualquier persona o grupo de personas por cualquier motivo (modo de expresión que cobija las categorías conocidas comúnmente como discurso del odio, discurso discriminatorio, apología del delito y apología de la violencia);* (c) la pornografía infantil; y (d) la incitación directa y pública a cometer genocidio.[47]

De estas citas se desprende que un elemento esencial del discurso de odio es la "incitación a la violencia" (la incitación a la discriminación está presente en algunos textos de derechos humanos, pero no en el inciso 5 de la Convención Americana).

---

46 CSJN, "Partido Nuevo Triunfo s/ reconocimiento - Distrito Capital Federal", 17 de marzo de 2009, disponible en: http://servicios.csjn.gov.ar/confal/ConsultaCompletaFallos.do?method=verDocumentos&id=663806

47 Corte Constitucional de Colombia, sentencia T-391/07, disponible en: http://bit.ly/1QF2hu2. El resaltado es propio.

Cabe preguntarse, entonces, si la pornografía no consentida, siendo en sí misma un supuesto de violencia de género que tiene su origen en la discriminación, debería además incitar a la violencia para poder ser considerada como un caso de discurso de odio.

La definición aquí brindada de pornografía no consentida podría inducir a pensar que no configuraría un supuesto de "incitación a la violencia", como sí podrían serlo los casos de acoso o de pornografía de venganza. No obstante, cumplidas ciertas condiciones, la pornografía no consentida configura un supuesto de discurso de odio por violencia de género.

Por un lado, la acción de pornografía no consentida podría estar acompañada de llamamientos explícitos a la violencia ilegítima contra la víctima. Ello configuraría un caso de discurso de odio, al estar motivado en un factor discriminatorio. Por ejemplo, podría presumirse que realizar una publicación del tipo de pornografía no consentida, en una plataforma abierta a comentarios públicos o semipúblicos, podría generar un caso de incitación a la violencia. Además, este supuesto podría configurar el delito previsto en el artículo 209 del Código Penal.[48]

Por otro lado, de acuerdo con la jurisprudencia de la Corte IDH, también podría considerarse que la acción de publicar o poner a disposición, que configuran la pornografía no consentida, es en sí misma un acto de violencia sexual contra las mujeres, de tipo psicológico. Entraría, entonces, dentro de las "acciones similares" a la incitación a la violencia.

En cualquiera de los dos casos estaría presente la violencia como elemento indispensable para permitir la restricción del contenido.[49]

3. ¿Cuál sería la consecuencia práctica de calificar a la pornografía no consentida como discurso no protegido?

3.1. Obligación del Estado de prohibir la pornografía no consentida

Una primera consecuencia es que se permitiría su prohibición, es decir, los Estados están obligados a garantizar esta proscripción. Esto no quiere decir

---

48 Código Penal de la Nación, Artículo 209: "El que públicamente instigare a cometer un delito determinado contra una persona o institución, será reprimido, por la sola instigación, con prisión de dos a seis años, según la gravedad del delito y las demás circunstancias establecidas en el artículo 41."

49 *Véase,* Organización de Estados Americanos, *Informe Anual de la Relatoría para la Libertad de Expresión 2004, capítulo 7,* párr. 46, disponible en: http://bit.ly/1Q9XfDc.

que se autorice su censura previa sino que se autoriza la prohibición previa por ley bajo apercibimiento de imposición de sanciones ulteriores,[50] dentro del marco muy limitado que la Convención Americana ofrece para restringir la circulación de contenido.[51]

Los reguladores podrían entonces prohibir la pornografía no consentida, cumpliendo los parámetros impuestos por la CIDH para la restricción de la libertad de expresión, esto es "previstas por ley, servir un fin legítimo establecido en el derecho internacional y ser necesarias para alcanzar ese fin".[52]

Esto es importante porque no son muchos los tipos de discursos que pueden prohibirse (la enumeración de la Corte Constitucional de Colombia que mencionamos anteriormente es acertada, son esos casos y ningún otro, no obstante lo cual amplía los supuestos del inciso 5).

En este sentido, los documentos de la RELE han indicado claramente que el Estado debe garantizar la libertad de expresión de las minorías. La pornografía no consentida es un obstáculo a la libertad de expresión de las víctimas.[53] Una de las consecuencias inmediatas de ser víctima de agresiones en internet es que la o el afectado tiende a desaparecer de la red (esto ya se ha visto con otros casos como *bullying*). La expresión de la víctima, sus opiniones, sus experiencias, la posibilidad de mostrar su identidad de la forma en que desee, son aniquiladas por el odio de su agresor.

Por ello la prohibición y remoción del contenido se presenta como una media necesaria. La RELE ha dicho que:

> 1. b. Los Estados deberían realizar acciones concretas y efectivas para modificar o eliminar estereotipos, prácticas y prejuicios nocivos, incluidos valores o prácticas tradicionales o consuetudinarios, que menoscaben la posibilidad de todas las personas y grupos en la sociedad de ejercer el derecho a la libertad de expresión. (…) d. Los Estados tienen cierto grado de flexibilidad conforme

---

50 *Ibíd.*, párrafo 29.

51 *Ibíd.*, párrafo 34.

52 Opinión Consultiva OC-5/85, párr 50, citada en Organización de Estados Americanos, *supra* nota 49, párrafo 34. La Corte IDH ha señalado que una comparación de los tres instrumentos demuestra que "las garantías de la libertad de expresión contenidas en la Convención Americana fueron diseñadas para ser las más generosas y para reducir al mínimo las restricciones a la libre circulación de las ideas."

53 Por el contrario, las leyes que regulaban el discurso de odio eran percibidas como una herramienta para acallar a las minorías, no para protegerlas. *Véase,* CIDH y otros, *Declaración conjunta del décimo aniversario: Diez desafíos claves para la libertad de expresión en la próxima década*, 2010, disponible en: http://bit.ly/1gvWs3K.

> al derecho internacional para decidir sobre la necesidad y, en su caso, el modo de restringir la libertad de expresión con el fin de proteger objetivos legítimos y, a la vez, respetar los estándares mencionados precedentemente, incluso para reflejar sus propias tradiciones, cultura y valores. El derecho internacional también reconoce que las diferentes situaciones que enfrentan los Estados en particular podrían ameritar distintos enfoques en lo que atañe a eventuales restricciones de la libertad de expresión. Ninguna de estas variaciones menoscaba en modo alguno el principio de universalidad de la libertad de expresión, y las restricciones a esta libertad en ningún caso deberían representar una imposición por determinados grupos de sus tradiciones, cultura y valores por sobre los de otros. (…) g. Los Estados deberían enfocarse particularmente, según lo ameriten las circunstancias locales, en combatir –lo cual incluye diseñar programas para contrarrestar– la discriminación histórica, los prejuicios y las actitudes tendenciosas impiden el goce igualitario del derecho a la libertad de expresión por ciertos grupos.[54]

Por otro lado, el Decreto 10/2010, reglamentario de la ley 26 485, en el artículo 6, inciso f, dispone que:

> Conforme las atribuciones conferidas por el artículo 9º incisos b) y r) de la Ley Nº 26.485, el CONSEJO NACIONAL DE LAS MUJERES dispondrá coordinadamente con las áreas del ámbito nacional y de las jurisdicciones locales que correspondan, las acciones necesarias para prevenir, sancionar y erradicar la difusión de mensajes o imágenes que:
> 1) Inciten a la violencia, el odio o la discriminación contra las mujeres. (...)
> 4) Contengan prácticas injuriosas, difamatorias, discriminatorias o humillantes a través de expresiones, juegos, competencias o avisos publicitarios.

Si bien la constitucionalidad de esta norma es cuestionable, ya que un organismo administrativo como el Consejo Nacional de las Mujeres no tiene facultades ni competencia para restringir la libre circulación de contenido, ni para determinar qué es discurso de odio, esta reglamentación podría ser una herramienta a través de la cual se determine expresamente que la pornografía no consentida es un caso de discurso de odio.

En este sentido, la Corte Suprema de Justicia de la Nación también ha dicho que: “La interdicción de la censura previa, en la Constitución Nacional, no llega al extremo de convertir al juez en mero espectador de un daño inexorable

---

54 CIDH y otros, *Declaración Conjunta sobre Universalidad y el Derecho* a *la Libertad de Expresión*, 2014*,* disponible en: http://bit.ly/1gvWs3K.

(voto de los Dres. Antonio Boggiano y Adolfo Roberto Vázquez)".[55], por lo cual los jueces también podrían calificar a la pornografía no consentida como un caso de discurso de odio y ordenar su remoción.

3.2. Facultad del Estado de remover el contenido (con orden judicial)

De todas maneras, aun calificando la pornografía no consentida como un supuesto de discurso de odio, resta establecer si la solicitud de la víctima a un intermediario de internet de restringir la circulación del contenido requiere o no de una orden judicial.

Los llamados "intermediarios de internet" son figuras muy importantes en relación con la publicación de contenido en internet ya que son quienes prestan un servicio técnico para que usuarios puedan publicar, distribuir o acceder a contenidos en internet.

Es importante determinar qué reglas debe seguir un intermediario a fin de resguardar la libertad de expresión (por supuesto, el autor del material puede removerlo sin necesidad de autorización alguna, pero una vez que ha sido publicado en la internet, en general escapa a su control que dicho material se torne inaccesible).

La RELE diseñó una serie de estándares para guiar al regulador en la implementación de un mecanismo legítimo de remoción de contenido en internet por parte de los ntermediarios de internet:

> No se debe exigir a los intermediarios controlar el contenido generado por usuarios y enfatiza la necesidad de protegerlos respecto de cualquier responsabilidad, siempre que no intervengan específicamente en los contenidos o cuando se nieguen a cumplir una orden judicial que exija su eliminación. La declaración expresa, además, que la competencia respecto de causas vinculadas con contenidos de internet debería corresponder exclusivamente a los Estados donde tales causas presenten impactos directos y genuinos.
> Asimismo, toda limitación a la libertad de expresión, incluyendo aquellas que afectan la expresión en internet, debe establecerse por ley de manera clara y precisa, debe ser proporcionada a los fines legítimos perseguidos y debe basarse en una decisión judicial fruto de un proceso contradictorio. En este sentido, la legislación sobre internet no debe incluir definiciones amplias y vagas, ni afectar de manera desproporcionada a sitios web y servicios legítimos.[56]

[55] CSJN, "S., V. c/ M. , D. A. s/ medidas precautorias", 03/04/2001, T. 324, P. 975.
[56] CIDH, Relatoría Especial para la Libertad de Expresión, *Declaración Conjunta sobre libertad*

De estos estándares surge que la RELE no ha admitido ningún supuesto de remoción privada de contenido sin orden judicial o de autoridad administrativa competente, con lo cual, esta solución está abierta al debate ya que numerosos proyectos de ley en la región pretenden establecer este mecanismo para casos de contenido "manifiestamente ilegítimo" (o conceptos similares).

En opinión de esta autora, una atenta lectura de los documentos del Sistema Interamericano y en particular de los emitidos por la RELE en relación a la libertad de expresión e internet, muestra que la remoción de contenido es una medida de responsabilidad ulterior permitida, pero en ningún caso, ni siquiera en el discurso de odio, puede removerse un contenido sin orden judicial o de autoridad competente.

No obstante, la calificación de discurso de odio permitiría inferir que no existirían supuestos de interés público que obligarían a resguardar el contenido. No hay interés público en casos de discurso de odio y no existiría motivo alguno para que el autor solicitara la publicación del contenido o la no remoción. Entonces, la remoción procedería una vez que el juez o la autoridad competente consideren configurado el supuesto, sin necesidad de balancear ningún otro derecho.

De todos modos, se advierte que, por ejemplo, el Marco Civil de Internet de Brasil no ha seguido esta línea de pensamiento. Dicha legislación condiciona la inmunidad de los proveedores de servicios de aplicaciones a que hagan cesar la puesta a disposición de material íntimo divulgado sin consentimiento, tan pronto como reciben una notificación con dicha solicitud por parte del afectado.[57] Es el único caso de dicho marco regulatorio en que no se exige notificación judicial.

---

de expresión en internet del Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión y la Relatora Especial para la libertad de expresión de la CIDH, 2012, disponible en: http://bit.ly/1TAf3wC.

57 Ley N. 12 695 de Marco Civil de Internet, Brasil, 23 de abril de 2014, disponible en: http://bit.ly/1jGz4fj, Art. 21: "El proveedor de aplicaciones de internet que ponga a disposición contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el afectado o su representante legal, dejare de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la puesta a disposición de ese contenido. Parágrafo único. La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido.". Traducción propia.

Por último, vale mencionar que la remoción estará sujeta a que efectivamente pueda eliminarse o bloquearse el material, lo que dependerá del tipo de tecnología que se hubiera utilizado para distribuirla. La distribución mediante SMS probablemente exigiría conocer quiénes fueron los destinatarios del material y extender la orden de remoción a estos sujetos. El calificar a la pornografía no consentida como discurso de odio tal vez permitiría superar la barrera de la confidencialidad de las comunicaciones.

3.3 Obligación de diligencia del Estado para prevenir, investigar, sancionar y reparar

Finalmente, se destaca que una consecuencia de calificar a la pornografía no consentida como un supuesto de violencia contra las mujeres es que el Estado tiene una obligación de diligencia para prevenir, investigar, sancionar y reparar estos actos.

La Corte IDH se refirió a esta obligación de forma reiterada en todas sus sentencias relativas a la violencia contra las mujeres:

> Es por ello que las autoridades estatales tienen la obligación de investigar *ex officio* las posibles connotaciones discriminatorias por razón de género en un acto de violencia perpetrado contra una mujer, especialmente cuando existen indicios concretos de violencia sexual de algún tipo o evidencias de ensañamiento contra el cuerpo de la mujer (por ejemplo, mutilaciones), o bien cuando dicho acto se enmarca dentro de un contexto de violencia contra la mujer que se da en un país o región determinada.[58]

También la Corte Constitucional de Colombia ha dispuesto que:

> Existe un marco jurídico por medio del cual el Estado despliega actuaciones afirmativas que pretenden garantizar el amparo de los derechos de las mujeres cuando son víctimas de violencia. Dicho marco sirve como presupuesto para el desarrollo de las distintas atribuciones a cargo de las autoridades públicas, así como de los particulares vinculados con el goce efectivo de sus derechos.[59]

58 Corte IDH. "Caso Véliz Franco y otros c/ Guatemala. Excepciones Preliminares, Fondo, Reparaciones y Costas", dentencia de 19 de mayo de 2014, disponible en: http://bit.ly/206ezyh.

59 Corte Constitucional de Colombia, sentencia T-434/14, disponible en: http://bit.ly/1nKE9go.

En la Argentina, el marco jurídico de los sistemas de derechos humanos está complementado por la ley 26 485. No obstante, como bien lo describe el informe de APC ya citado:

> La VCM relacionada con la tecnología se sitúa dentro de una cultura de impunidad, que se caracteriza por una falla en la aplicación de los procesos legales, y la percepción de que los actos de VCM quedan impunes. La investigación descubrió que existía una cultura de impunidad en casos de VCM relacionada con la tecnología en los siete países estudiados. Esto a menudo se ve agravado por la corrupción del sistema judicial y la falta de voluntad política para encarar la problemática de la VCM.[60]

No solo el desconocimiento sobre las medidas concretas de protección sino la percepción de impunidad a favor del agresor, desmotivan la denuncia. En este caso, el problema de la pornografía no consentida es invisibilizado por el mismo Estado que no ha desarrollado herramientas concretas de detección y protección.

Una de las medidas necesarias para una protección eficaz es la generación de estadísticas:

> "La exigencia de un sistema de estadísticas sobre actos de violencia contra las mujeres, ha sido enfatizada igualmente por órganos del Sistema Universal de Derechos Humanos y del Sistema Interamericano de Derechos Humanos, que han recabado en la necesidad de contar con información sobre la vulneración de los derechos humanos de la mujeres, como una herramienta para el diseño e implementación de políticas y medidas de prevención efectivas. Además, el conocimiento sobre los hechos violatorios de derechos humanos, constituye un derecho de las víctimas y de la sociedad en general, de modo que: "[l]os Estados tienen también el deber de crear y preservar archivos públicos destinados a recopilar y sistematizar la información referida a graves violaciones de derechos humanos padecidas en los países." Por otra parte, el deber de debida diligencia es a su vez consistente con la obligación internacional de los Estados de proveer un recurso judicial efectivo, que permita a los ciudadanos y ciudadanas la posibilidad real de solicitar ante las autoridades competentes: (i) la declaración de que un derecho está siendo vulnerado, (ii) el cese de la vulneración y (iii) la reparación adecuada por los daños causados.[61]

---

60 APC, *Explorando soluciones corporativas y legales contra la violencia hacia las mujeres relacionada con la tecnología,* disponible en: http://bit.ly/1SVZ24L.

61 Corte Constitucional de Colombia, Auto 009/15, disponible en: http://bit.ly/1NOEjrK.

Otra de las medidas es el acceso a la justicia, que implica establecer procedimientos que generen confianza en la víctima. El Decreto 10/2010 lo ha establecido claramente:

> inciso f).- El acceso a la justicia a que hace referencia la ley que se reglamenta obliga a ofrecer a las mujeres víctimas de violencia todos los recursos necesarios en todas las esferas de actuación del ESTADO NACIONAL, ya sean de orden administrativo o judicial o de otra índole que garanticen el efectivo ejercicio de sus derechos.
> El acceso a la justicia comprende el servicio de asistencia jurídica gratuita, las garantías del debido proceso, la adopción de medidas positivas para asegurar la exención de los costos del proceso y el acceso efectivo al recurso judicial.

El acceso a la justicia implica, al igual que con cualquier otro supuesto de violencia de género, el establecimiento de instituciones, en los tres poderes del Estado, preparados para dar respuestas adecuadas. Por ejemplo, la oficina de Violencia Doméstica de la Corte Suprema de Justicia de la Nación podría ser un organismo apto para recepcionar este tipo de denuncias y emitir, de forma inmediata, una orden de remoción del contenido. Otra cuestión que podría incluirse entre los procedimientos de violencia doméstica o entre las cuestiones a resolver en un proceso de divorcio es la tenencia o destrucción de material íntimo producido de común acuerdo.[62] A este fin es fundamental superar las actitudes de juzgamiento por parte de los oficiales públicos y poder hacer las preguntas concretas para proveer las soluciones adecuadas.

> Ante este contexto, la administración de justicia no puede convertirse en otra instancia para la transferencia de responsabilidad o de normalización del empleo de estereotipos o prejuicio en la operación de la administración de justicia. Quienes denuncian, deben poder confiar en un sistema jurídico libre de estereotipos y en un poder judicial cuya imparcialidad no se vea comprometida por suposiciones sesgadas.[63]

[62] "En Europa, una Corte alemana resolvió en mayo que las fotografías íntimas de una pareja debían ser eliminadas si así ésta lo solicita. La decisión de la Corte Suprema Alemana se produjo luego de que un hombre divorciado se negara a eliminar las imágenes eróticas de su ex esposa luego de la ruptura. El fue llevado a juicio por su ex esposa quien ganó el caso y obtuvo la eliminación de las fotos". Simpson, Jack, "*Revenge porn, what is it and how widespread is the problem",* en: The Independent, 2 de julio de 2014, disponible en: http://ind.pn/1J2Ea4H.

[63] Corte Constitucional de Colombia, sentencia 634-13, disponible en: http://bit.ly/1OyMApE.

Al no estar habilitada por el Sistema Interamericano la remoción privada de contenido, el acceso fácil y expedito a la justicia es la mejor solución ya que es la alternativa que supera todo tipo de debates y puede resguardar todos los derechos involucrados.

En términos procesales, el artículo 43 de la Constitución[64] garantiza la acción de amparo contra "actos de particulares" que lesionen derechos fundamentales, si no existiera otro medio judicial más idóneo. Si consideramos a la violencia de género como un caso de discurso de odio, la acción de amparo sería el remedio judicial más idóneo.

Finalmente, sin adentrarnos demasiado en la reparación por vía de indemnización por daños y perjuicios, sí parece relevante destacar las normas del Código Civil y Comercial de la Nación, aplicables a esta situación: en primer lugar, el deber genérico de no dañar a otro. Si bien se ha expresado antes que la configuración del supuesto de pornografía no consentida no requiere la intención de provocar un daño, eso no quiere decir que no se produzca daño. En todos los casos en que ocurre este supuesto ocurre un daño, aun cuando el autor no haya tenido esa intención. Por lo tanto, surge el deber de reparar establecido en el artículo 1716.[65]

Pero también debe destacarse que el artículo 1719 descarta que la "asunción de riesgos" por parte de la víctima (como podrían interpretar algunos jueces lo es el consentimiento para la producción del material), la prive de la reparación del daño.

Por ejemplo, la reparación de los daños y perjuicios por la publicación de material íntimo fue ordenada en Chile[66] y extendida a los padres del menor que filmó y divulgó el contenido por no haberlo denunciado o evitado. Este caso bien podría incluirse en la definición de pornografía no consentida

---

64 Constitución Argentina, Art. 43, "Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. Podrán interponer esta acción contra cualquier forma de discriminación (…)".

65 Código Civil y Comercial de la Nación, Art. 1716, "Deber de reparar–. La violación del deber de no dañar a otro, o el incumplimiento de una obligación, da lugar a la reparación del daño causado, conforme con las disposiciones de este Código"; Art. 1719, "Asunción de riesgos-. La exposición voluntaria por parte de la víctima a una situación de peligro no justifica el hecho dañoso ni exime de responsabilidad a menos que, por las circunstancias del caso, ella pueda calificarse como un hecho del damnificado que interrumpe total o parcialmente el nexo causal".

66 *Véase,* CNN Chile, "Autor de video 'wena Naty' deberá pagar indemnización de 35 millones", 25 de abril de 2015, disponible en: http://bit.ly/1EE1ffl.

objeto de este estudio, ya que el menor que capturó y divulgó las imágenes (ambas acciones sin consentimiento de la víctima) estaba participando de la actividad sexual. Es decir, integra un concepto amplio de "pareja".

En relación con la potencial responsabilidad de los medios de prensa que pudieran reproducir este tipo de material, la Corte Suprema ha establecido el estándar de la "negligencia precipitada" o "simple culpa" para los casos en que no existe un interés público involucrado en la publicación:

> 11) Que de tal modo y aun considerando que frente a la difusión de asuntos de interés público, la posibilidad de reprimir los juicios que pudieran tener contenido difamatorio sólo podría hallarse justificada en un muy estrecho margen, la protección que merecen los particulares del caso en cuanto a su honor, obligaba a una mayor prudencia, bastando la "negligencia precipitada" o "simple culpa" en la propalación de imágenes o referencias de los demandantes antes nombrados para generar la condigna responsabilidad de la demandada.[67]

También ha dicho la Corte Suprema en el caso "Irigoyen Juan Carlos Hipólito c/ Fundación Wallemberg s/ Ds y Ps.",[68] del 5 de Agosto de 2014, que corresponde aplicar la doctrina "Campillay" para el caso de páginas web que publican contenido de terceros y la doctrina de la real malicia cuando el contenido publicado es propio, indicando que en este caso la real malicia no se configura en el caso de las "hipérboles" sino que "en el ámbito de los 'juicios de valor' lo único prohibido es caer en el 'insulto' o en la 'vejación gratuita o injustificada'". Es decir, se aplicaría la doctrina de la real malicia si el medio, tomado en sentido amplio (¿tal vez un blog?), decidiera publicar pornografía no consentida (sabiendo o debiendo saber que no es consentida), ya que constituiría una vejación injustificada (de nuevo, si es o no injustificada dependerá de la calificación legal que se le otorgue, es decir si se permiten excepciones de interés público o no).

En relación con los intermediarios de internet, no existe en Argentina, como sí en otras partes del mundo, una ley que limite su responsabilidad por el contenido dañoso generado y publicado por los usuarios. La Corte Suprema de Justicia de la Nación resolvió en el caso "Rodríguez, María Belén c/

---

67 CSJN, "Barrantes Juan Martin – Molinas de Barrantes Teresa - TEA S.R.L. c/ Arte Radiotelevisivo Argentino S.A. y ot./ Sumario", 1/8/2013, disponible en: http://bit.ly/1maHvro.

68 CSJN, "Irigoyen Juan Carlos Hipólito c/ Fundación Wallemberg s/ Ds y Ps.", 5 de Agosto de 2014, disponible en: http://bit.ly/1PdKiZe. También disponible con con comentarios por Paula Vargas, en: http://bit.ly/1SqzSvz.

Google Inc. y ot. s/ Ds. y Ps."[69] que los motores de búsqueda son responsables a partir de que toman conocimiento –mediante una notificación válida– del contenido dañoso, momento en que surge la obligación de removerlo.

En Estados Unidos, por ejemplo, en el año 1996 se sancionó la Communications Decency Act[70] para regular el contenido indecente en internet. Esta ley fue declarada inconstitucional por violar la Primera Enmienda, pero la Corte Suprema dejó subsistente una sola norma: la que concede inmunidad absoluta a los intermediarios de internet por el contenido indecente publicado por sus usuarios (siempre que no vulnere propiedad intelectual, no constituya un delito federal, o no vulnere derecho estatal). Paradójicamente, quienes más han defendido esta ley, modelo de libertad de expresión, se encuentran ahora con que la misma es también un obstáculo para detener la pornografía no consentida, que unánimemente consideran como discurso no protegido.

En opinión de esta autora, esta situación de no poder compeler a los intermediarios (aunque la gran mayoría se ha autorregulado y acepta remover este contenido), en particular a los que crean plataformas para que deliberadamente se publique pornografía no consentida, es lo que ha desatado la ola criminalizadora en varios Estados de los Estados Unidos. No son muchas las voces que se alzan contra el CDA, que ha probado ser una ley equilibrada, pero la pornografía no consentida pareciera ser una bisagra, véase en este sentido la durísima opinión de Ann Bartow en su post "Acoso en línea, ánimo de lucro y la Sección 230".[71]

En conclusión, la pornografía no consentida, de acuerdo a la definición aquí elaborada, podría encuadrarse dentro de la clasificación de discurso de

---

69 CSJN, "Rodríguez María Belén c/ Google Inc. y ot. s/ Ds y Ps", 28 de Octubre de 2014, disponible en: http://bit.ly/1UGGjrD.

70 47 U.S., Code Section 230, disponible en: http://bit.ly/1hlnlbP.

71 La oposición a modificar la Sección 230 ha sido feroz, porque cumplir con las regulaciones gubernamentales siempre cuesta dinero. Esta oposición no es para nada ingenua: la línea argumental de los ISP [proveedores de servicios de internet], fuertemente proclamada y muy útil para ellos mismos, es que sin la Sección 230, los monstruos de internet como Google, Yahoo, Bing, Facebook, Youtube y Twitter no existirían. Citron aparentemente acepta esta postura. Pero yo no la creo por un segundo, y ustedes no deberían tampoco. (…) [T]odas estas compañías hacen negocios en países que no tienen leyes de inmunidad. La Sección 230 les ahorra a los ISP dinero. Este es el real valor para ellas. Les evita el deber de proteger, compensar o siquiera interactuar con personas que han sido dañadas por los bienes y servicios que producen. Éstas lo aman, pero no lo necesitan (a pesar de que claman en sentido contrario). Las empresas de internet funcionan y muchas veces cosechan enormes ganancias en todo el mundo sin ninguna ley similar a la Sección 230. Están dispuestas a arriesgarse por el dinero." Bartow, Ann, *Online Harassment, Profit seeking, and Section 230,* en: *Boston University Law Review*, 2 de Noviembre de 2015, disponible en: http://bit.ly/1NOEjYM. Traducción propia.

odio, por configurar un supuesto de incitación a la violencia contra las mujeres. Esto habilitaría ciertas consecuencias legales –como el deber del Estado de prohibir este contenido– y de protección que no están disponibles para otras figuras jurídicas.

Vale aclarar, por último, que regular con el estándar de género brinda una mayor protección, de la que también se beneficiaría una víctima que no fuera mujer biológicamente (en este grupo podrían entrar otros grupos víctimas de violencia de género como las personas trans); no es relevante el sexo de quien comete el acto (podría tratarse de una ex pareja mujer) sino que lo relevante es que el contenido de la pornografía no consentida, típicamente, humilla a las mujeres (cuánto más podría hacerlo en sociedades conservadoras si además fuera una relación homosexual).

No obstante, como lo indica la resolución 505/2013 del Ministerio de Seguridad que establece las Pautas para la intervención policial en casos de violencia en relaciones familiares: "Atento a la magnitud de la violencia que padecen en nuestro país niños, niñas, adolescentes y mujeres mayores, el presente instrumento tendrá como eje la situación de las mujeres y se harán precisiones cuando sea necesario para otras poblaciones".[72]

4. La pornografía no consentida como una vulneración del derecho a la privacidad

Otra perspectiva posible para regular la pornografía no consentida es el derecho a la privacidad, que es un derecho fundamental consagrado en los pactos de derechos humanos con rango constitucional, así como en la Constitución Nacional. También regula la privacidad el Código Civil y Comercial de la Nación[73] y el artículo 31 de la ley 11 723 de Derechos de autor.

---

72 MSAL, resolución 505/2013, "Pautas para la Intervención Policial en casos de violencia en relaciones familiares", 31 de mayo de 2013, disponible en: http://bit.ly/1Q9Y52R.

73 Código Civil y Comercial de la Nación: ARTICULO 51.- Inviolabilidad de la persona humana. La persona humana es inviolable y en cualquier circunstancia tiene derecho al reconocimiento y respeto de su dignidad. ARTICULO 52.- Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1. ARTICULO 53.- Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos

En particular el Código Civil ha hecho referencia a la publicación "arbitraria":

> "ARTÍCULO 1770.- Protección de la vida privada. El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias. Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación."

La privacidad, en sentido genérico, comprende el derecho al honor, a la intimidad, a la propia imagen y también a la protección de los datos personales (aunque este es también considerado como un derecho fundamental independiente en el Sistema Europeo de Derechos Humanos, sin que esté claro si el Sistema Interamericano también lo considera como un derecho distinto o lo subsume en el derecho a la privacidad).

La jurisprudencia de la Corte IDH ha resuelto que la vida privada es parte de la protección a la "honra y la dignidad", y en particular, la vida sexual de una persona es parte de su privacidad:

> "Por otro lado, la Corte ha precisado que si bien el artículo 11 de la Convención Americana se titula 'Protección de la honra y de la dignidad', su contenido incluye, entre otros, la protección de la vida privada. El concepto de vida privada comprende entre otros ámbitos protegidos, la vida sexual".[74]
> "En cuanto a la alegada violación del artículo 11 de la Convención Americana, en base a los mismos hechos, el Tribunal ya ha precisado que el contenido de dicha norma incluye, entre otros, la protección de la vida privada. Por su parte, el concepto de vida privada es un término amplio no susceptible de definiciones exhaustivas, pero que comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos".[75]

---

de interés general."

74 Corte IDH, "Caso Masacres de Río Negro c/ Guatemala. Excepción Preliminar, Fondo, Reparaciones y Costas", sentencia del 4 de septiembre de 2012, párrafo 133. En el mismo sentido, *véase,* Corte IDH, "Caso Gudiel Álvarez y otros (Diario Militar) c/ Guatemala. Fondo, Reparaciones y Costas", sentencia del 20 de noviembre de 2012, párrafo 276.

75 Corte IDH, "Caso Masacres de El Mozote y lugares aledaños c/ El Salvador. Fondo, Reparaciones y Costas", sentencia de 25 de octubre de 2012, párrafo 166.

> El ámbito de protección del derecho a la vida privada ha sido interpretado en términos amplios por los tribunales internacionales de derechos humanos, al señalar que éste va más allá del derecho a la privacidad. La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad.[76]
>
> La afectación de los derechos fundamentales en redes sociales como Facebook puede ocurrir no sólo respecto de la información que los usuarios de esta red social ingresan a la misma o cuyo ingreso permiten a través de su perfil, sino también con relación a información de personas, usuarias o no, que ha sido publicada y usada por terceros en las redes sociales. Ante los usos que pueden darse en las redes sociales de la propia imagen, un contenido mínimo del derecho a la imagen es la posibilidad de excluirla de las redes, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular. Lo anterior encuentra fundamento en la protección constitucional debida a la imagen como expresión directa de la individualidad, identidad y dignidad de las personas. En este sentido, la disponibilidad de la propia imagen exige la posibilidad de decidir sobre su cambio o modificación, lo cual constituye a su vez un presupuesto ineludible del ejercicio del libre desarrollo de la personalidad. (...) Orden a empresa de masajes proceda a retirar de la red social Facebook y de cualquier otro medio de publicidad las imágenes y se abstenga en el futuro de divulgar y publicitar las fotografías de la accionante.[77]

Nótese que este fallo dirige la orden de remoción contra quien publicó el contenido en la plataforma Facebook, no a Facebook.

---

[76] Corte IDH, "Caso Artavia Murillo y otros (Fecundación in vitro) c/ Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas", sentencia de 28 de noviembre de 2012, párrafo 143.

[77] Corte Constitucional de Colombia, sentencia 634-13, disponible en: http://bit.ly/1OyMApE.

¿Cuál sería la diferencia en términos prácticos si la pornografía no consentida se regulara como un supuesto de violación de la privacidad y no, por ejemplo, con un caso de discurso de odio?

El derecho a la libertad de expresión en cierta forma se fortalece y el balance entre ambos derechos requiere necesariamente la intervención judicial o de una autoridad competente para cumplir el objetivo que en general tienen las víctimas que es lograr remover el contenido (sea por parte del autor o de un intermediario de internet). Así lo dispone el artículo 1 770 del Código Civil y Comercial Argentino, citado anteriormente, que menciona que el cese del acto arbitrario de intromisión en la vida privada y la indemnización deben ser ordenadas por un juez.

Resulta entonces que al igual que en el caso del discurso de odio, cualquier restricción a la libertad de expresión para resguardar la privacidad debería ser ordenada por un juez o una autoridad administrativa competente pero, a diferencia del discurso de odio, no podría existir una prohibición de este discurso e imperiosamente el juez de forma previa a ordenar la remoción debería hacer un balance de derechos entre la privacidad y la libertad de expresión.

Ya se dijo anteriormente que en el caso del discurso de odio, ningún balance es debido. Al fortalecerse el derecho a la libertad de expresión, se fortalece también la necesidad de prever excepciones por cuestiones de interés público. No obstante, debe considerarse con sumo cuidado esta excepción para no revictimizar a la víctima.

Debería aplicarse una interpretación muy restrictiva como para permitir que una pareja o ex pareja publique contenido íntimo y que este deba circular por razones de interés público. Obviamente, deberá estar vinculado a alguna causal que no sea la mera exhibición de la vida privada o la estigmatización de la conducta de un funcionario o una persona pública.

En el mismo sentido, la Corte Suprema de Justicia de la Nación en el fallo "Rodríguez María Belén c/Google Inc. y ot. s/ Ds y Ps"[78] (2013) encuadró el caso de la remoción de vínculos, por parte de los motores de búsqueda, a páginas que vulneraban el derecho al honor de la actora, como un "balance entre libertad de expresión y derecho a la privacidad" y resolvió que los motores de búsqueda están obligados a remover el contenido dañoso desde que son notificados por parte de la víctima.

En relación a la validez de la notificación, aspecto crítico para determinar cuándo la víctima adquiere el derecho a que se remueva el contenido, la Corte

---

[78] CSJN, *supra* nota 69, párrafo 18.

Suprema ofrece un estándar *obiter dictum* (esto es muy importante recalcarlo, no es un estándar vigente y no ha sido testeado en relación con los estándares de libertad de expresión del Sistema Interamericano).

Dijo la Corte Suprema que:

> Son manifiestas las ilicitudes respecto de contenidos dañosos, como pornografía infantil, datos que faciliten la comisión de delitos, que instruyan acerca de éstos, que pongan en peligro la vida o la integridad física de alguna o muchas personas, que hagan apología del genocidio, del racismo o de otra discriminación con manifiesta perversidad *o incitación a la violencia*, que desbaraten o adviertan acerca de investigaciones judiciales en curso y que deban quedar secretas, como también los que importen lesiones contumeliosas al honor, montajes de imágenes notoriamente falsos o que, en forma clara e indiscutible, importen violaciones graves a la privacidad exhibiendo imágenes de actos que por su naturaleza deben ser incuestionablemente privados, aunque no sean necesariamente de contenido sexual. La naturaleza ilícita –civil o penal– de estos contenidos es palmaria y resulta directamente de consultar la página señalada en una comunicación fehaciente del damnificado o, según el caso, de cualquier persona, sin requerir ninguna otra valoración ni esclarecimiento. Por el contrario, en los casos en que el contenido dañoso que importe eventuales lesiones al honor o de otra naturaleza, pero que exijan un esclarecimiento que deba debatirse o precisarse en sede judicial o administrativa para su efectiva determinación, cabe entender que no puede exigirse al 'buscador' que supla la función de la autoridad competente ni menos aún la de los jueces. Por tales razones, en estos casos corresponde exigir la notificación judicial o administrativa competente, no bastando la simple comunicación del particular que se considere perjudicado y menos la de cualquier persona interesada.[79]

Como se mencionó al desarrollar la perspectiva del discurso de odio, el Sistema Interamericano no admitiría la remoción de contenido sin orden judicial o de autoridad administrativa competente. Sin embargo, en el caso de la incitación a la violencia se anularía la posibilidad de que exista un interés público involucrado, pero la vulneración de la privacidad requiere la intervención de una autoridad que efectúe el balance de derechos y resguarde el interés público.

---

[79] *Ibíd.*

Por supuesto, la indemnización por daños y perjuicios y la utilización de la vía del amparo establecida en el artículo 43 de la Constitución Nacional serían aplicables al igual que en el caso del discurso de odio, ya que la privacidad es igualmente un derecho fundamental.

Pero además, la perspectiva de la pornografía no consentida aportaría otra herramienta procesal que es el hábeas data, contemplado en el artículo 43 de la Constitución Nacional y en particular en la Ley 25 326 de Protección de datos personales. Sin pretender ingresar aquí en el arduo debate del llamado "derecho al olvido", la imagen es un dato personal y la falta de consentimiento al tratamiento de dicho dato podría dar derecho al ejercicio del derecho de oposición. En ese caso – excepto que se tratara de un diario (por la inmunidad de las bases de datos periodísticas) o que no se considere a los intermediarios de internet como "responsables del archivo"–, la víctima tendría derecho a exigir directamente al autor la remoción, o solicitarlo judicialmente mediante la acción de hábeas data.

No obstante, como la protección de los datos personales no es un derecho absoluto, deberá balancearse con el derecho a la libertad de expresión. Si bien la ley 25 326 concede al titular del dato el derecho a oponerse al tratamiento o a solicitar la cancelación del dato, en el caso de contenido publicado por usuarios de un servicio de los intermediarios de internet, las reglas a seguir deberían ser las de la RELE explicitadas más arriba (remoción previa orden judicial o de autoridad administrativa competente).

IV. La criminalización de la pornografía no consentida

La tendencia regulatoria en el mundo occidental, y en algunos países de Oriente es a convertir la pornografía no consentida, o alguna de sus variantes, (pornografía de venganza o acoso) en un delito o al menos en una falta (*misdemeanor*), sustrayendo la reparación o sanción del ámbito meramente civil.

El argumento para criminalizar es que, ante el enorme daño que provoca la pornografía no consentida y la dificultad para contener dicho daño una vez que la publicación ha ocurrido, por ejemplo en internet, la única herramienta realmente eficaz en términos preventivos sería la sanción penal.

En 2009, Filipinas fue el primer país en criminalizar la pornografía no consentida. En 2013 fue criminalizada por el Estado de Victoria, en Australia y Australia misma está ahora debatiendo una ley nacional. En 2014, Israel y Canadá introdujeron este delito en sus legislaciones. Gales e Inglaterra

criminalizaron esta conducta en el año 2015 y Japón también en el mismo año. En América Latina hay proyectos de ley en Brasil, Uruguay y Argentina[80].

En los Estados Unidos, la gran mayoría de los Estados han aprobado leyes anti-*revenge porn,* si bien no existe aún una ley federal que regule la cuestión. Estas regulaciones oscilan entre la criminalización como un delito o como un *misdemeanor* y presentan también variantes en cuanto a la acción contemplada.[81] Los activistas procriminalización han criticado a aquellas que exigen una determinada intención (causar daño), porque restringe su aplicación. En California ya se obtuvo la primera condena.[82] Es interesante que en este caso, además de la publicación de las imágenes y de los agravios a la víctima (por supuesto, utilizando la actividad sexual como motivo de agravio), el agresor instaba a su empleador a despedirla (lo cual es una incitación a la violencia según nuestra definición).

También fue condenado –a 18 años de cárcel– el administrador de una página web creada específicamente para propósitos de pornografía de venganza, pese que en los Estados Unidos los intermediarios de internet tienen inmunidad por los daños derivados del contenido generado por usuarios. No obstante, este administrador realizaba una especie de maniobra extorsiva para remover el contenido que fue considerada al momento de condenarlo.[83] Es decir no se lo condena por ser intermediario, sino por sus propias acciones.

España incorporó la figura de la pornografía no consentida a través del artículo 197.7:

> Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del

---

80 Para los proyectos de ley de argentina *véase*: HCDN, Código penal: incorporación de los artículos 139 ter, 149 quater y 157 ter, sobre robo de identidad, disponible en: http://bit.ly/1NOEi7n; HCDN, Violencia mediática: modificación de las leyes 26485 y 26522, disponible en: http://bit.ly/1o2XUzG; HCDN, Tratamiento mediático de la violencia de género: régimen, disponible en: http://bit.ly/1X0wExz; HCDN, Código Penal: modificación de los artículos 153 y 155, sobre uso, apertura y publicación de imágenes o videos audiovisuales, disponible en: http://bit.ly/206fMWe.

81 *Véase,* Goldberg*, State Revenge Porn Laws,* disponible en: http://bit.ly/1I0SSIy.

82 BBC news, *Revenge Porn Facebook post leads to jail sentence,* 3 de diciembre de 2014, disponible en: http://bbc.in/1ykojum.

83 Méndez Manuel Ángel, “18 años de cárcel para el administrador de una página de *revenge porn”,* en: Gizmodo, 4 de abril de 2015, disponible en: http://bit.ly/1SVZD6z.

> alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.
> La pena se impondrá en su mitad superior [hasta 7 años de cárcel si hay fines lucrativos, según artículo 197.6, y afecta a los tipos de datos mencionadas en el artículo 197.5] cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.[84]

Como se observa, es un tipo penal amplio, mucho más restrictivo de la libertad de expresión que el concepto aquí propuesto como pornografía no consentida, que podría eventualmente servir de base a un tipo penal.

La Cámara de Representantes de Puerto Rico aprobó un proyecto de ley contra la "pornografía de venganza"[85] que criminaliza y sanciona fuertemente varias acciones en torno al contenido. La ley está siendo debatida en el Senado con expresiones a favor y en contra.[86]

Como se mencionó antes, Israel también criminalizó la pornografía de venganza,[87] *acto al que calificó como un delito sexual*. Esto se aparta de las otras regulaciones, pero tiene sentido si, por ejemplo, se entiende a la pornografía no consentida como un supuesto de violencia sexual motivada por razones de género.

Desde la perspectiva académica, en los Estados Unidos la más acérrima defensora de la criminalización ha sido la autora ya mencionada, Danielle Citron, quien ha arengado incansablemente a favor de criminalizar la pornografía de venganza. Considera esta profesora de la Universidad de Maryland que las sanciones civiles no disuaden al autor y que solo la amenaza de prisión efectiva puede detener este flagelo.

Debe destacarse aquí que Citron advoca por la criminalización o la ampliación de la figura del acoso[88], que excede a la cuestión de la pornografía no

---

84 Código Penal de España, enero 2016, disponible en: http://bit.ly/1zOpvmz.

85 *Véase*, Ley contra la veganza pornográfica en Puerto Rico, disponible en: http://bit.ly/1QF3KAL.

86 *Véase,* Estrada Torres, Michelle, "Mirada multidisciplinaria al proyecto de ley de pornovenganza", en: El Nuevo Día, 10 de abril de 2015, disponible en: http://bit.ly/1nDs1x9.

87 Azulay Moran, "*Knesset outlaws revenge porn",* en: YNetnews.com, 1 de junio de 2014, disponible en: http://bit.ly/1KUzFbW.

88 "Actualmente, muchas leyes de acoso o de acecho no incluyen las amenazas de violación o la publicación de fotos de la víctima desnuda en los blogs o páginas web del acosador, o las publicidades falsas que ofertan un presunto interés de la victima en mantener relaciones sexuales

consentida. En su argumentación, la pornografía no consentida es una manifestación de conductas de acoso o abuso, todas las cuales, a su criterio, merecen ser criminalizadas. Esta opinión también debería ser considerada por los reguladores que lean la presente investigación, pero no abordaremos aquí la conveniencia o no de criminalizar otras conductas que no sea estrictamente la definición que hemos dado de pornografía no consentida.

En América Latina, Pablo Palazzi también ha propuesto la criminalización de la pornografía no consentida,[89] de una forma amplia; esto es, incluyendo supuestos que exceden la publicación o puesta a disposición por parte de una persona con una relación íntima con la víctima. Expresa Palazzi que son tres los fundamentos legales que habilitan a criminalizar estas conductas:

> El primer fundamento de la propuesta que realizamos en esta nota es el derecho a la intimidad de las personas cuya imagen es difundida sin permiso. (…) En segundo lugar, cabe hacer mención también de la Ley 24 632 que aprueba la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (conocida como "Convención de Belem do Pará"). (...) El tercer argumento es un argumento negativo, relativa a la falta de interés público en la publicación o difusión de estas imágenes que forman parte de la vida privada de las personas. Nadie puede argumentar un interés legítimo alguno para difundirlas (la libertad de expresión en este caso debe ceder frente a la privacidad del contenido).[90]

También indica que el delito a tipificar podría concurrir con los delitos ya regulados por los artículos 153 y 153 bis del Código Penal para el caso en que la imagen haya sido captada sin el consentimiento de la víctima.

También la Convención de Estambul propone la criminalización del acoso, al que considera una forma de violencia contra las mujeres. Es relevante la aclaración de que pese a la falta de datos "es bien conocido que muchas de

---

con desconocidos o las mentiras difamatorias que aparecen en muros de mensajes. Estas conductas no están alcanzadas porque el abuso no está directamente comunicado a la víctima. Pero las leyes de acecho y acoso deberían cubrir cualquier mecanismo, método o tecnología utilizada por los agresores para perseguir a sus víctimas. Los fiscales deberían tener la posibilidad de presentar la totalidad del abuso; esta totalidad, después de todo, es la que pone en peligro la vida, la salud y las carreras de las víctimas". Citron, Danielle, "*Expand harrassment laws to protect victims of online abuse",* en: Aljazeera America, 21 de marzo de 2015, disponible en: http://bit.ly/1PdL2xq.

89 Palazzi, Pablo, "Introducción al problema del *Revenge Porn",* en: *Derecho de Internet y Tecnología de las Comunicaciones*, *Working Paper Series* N. 1, 31 de Agosto de 2015, disponible en: http://bit.ly/1KUzKwf.

90 *Ibíd.*

las víctimas son mujeres y muchos de los perpetradores hombres". Apunta a criminalizar la actitud sostenida en el tiempo y no los actos aislados pero advierte que:

> (…) los procedimientos criminales pueden no detener a un acosador, por lo cual es necesarios garantizar la seguridad de la víctima. La Convención se asegura que un Tribunal pueda ordenar al acosador que cese en su comportamiento y se aleje de la víctima. Cualquier violación de dichas órdenes deben ser sancionadas criminalmente o mediante otras sanciones legales.[91]

Precisamente, el reconocer que los procedimientos criminales no detienen la conducta es lo que hace dudar de la necesidad de sancionar penalmente como si esta fuera una solución efectiva. Como ya sabemos en la Argentina, tampoco lo son las órdenes de restricción en caso de violencia doméstica, pero tal vez podría funcionar un procedimiento restrictivo para el caso de amenazas de pornografía no consentida.

No obstante, por ejemplo la Corte Constitucional de Colombia ha expuesto como argumento que la criminalización de los actos de violencia de género o doméstica (lo que sucede cuando la violencia la ejerce una pareja) protegen como bien jurídico a la familia, no a la integridad física.[92] Es decir, existe un bien jurídico a proteger que es más amplio que la necesidad de resguardar la integridad física o psicológica de la víctima. Por ello, si se lo considera desde esta perspectiva, el análisis la efectividad o no de la criminalización como medida preventiva puede arrojar otros resultados.

Sea por ineficacia o por los abusos a los que puede llevar, existen argumentos para ser cautos antes de crear nuevos tipos penales. Como lo expresa elocuentemente Sarah Jeong para Wired:

> El problema de la pornografía de venganza está inserto dentro de un contexto mayor de violencia contra las mujeres y de estigmatización del cuerpo desnudo, lo que significa que el problema puede ser abordado desde muchas

---

91 *Ibíd.*

92 "En este caso, el bien jurídico tutelado por el tipo penal definido en el artículo 229 de la Ley 599 de 2000 es la familia, de tal forma que si la violencia, sea cual fuere el mecanismo para infligirla, trae como consecuencia la afectación de la unidad y armonía familiar, rompe los vínculos en que se fundamenta esta estructura esencial de la sociedad, habrá antijuridicidad, elemento necesario para sancionar penalmente la conducta, por cuanto no es la integridad física el bien jurídicamente protegido por este infracción penal".Corte Constitucional de Colombia, sentencia C-368/14, disponible en: http://bit.ly/1VHoNnw.

> otras perspectivas. ¿Por qué regular internet cuando las órdenes de restricción no se pueden hacer cumplir, cuando las mujeres encuentran un montón de obstáculos para iniciar acciones civiles contra sus abusadores, cuando los empleadores pueden despedir a una empleada por ser un objeto sexual en internet? Nuestros esfuerzos regulatorios serían más productivos si se dirigieran a paliar el sufrimiento de las víctimas.[93]

En Argentina, la criminalización de la discriminación no fue considerada como una solución efectiva, de acuerdo al informe del INADI (Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo).[94] Si bien el supuesto de la pornografía no consentida no fue parte de la encuesta y excede lo que es la discriminación, puede servir como parámetro de la opinión social frente a la acción punitiva del Estado.

También se ha opinado contra la criminalización extendida a supuestos que no incluyen estrictamente a la pareja de la víctima. Voces relevantes en el debate sobre derechos civiles y libertad de expresión, como las de la Unión Estadounidense por las Libertades Civiles (ACLU, por su nombre en inglés) y Mary Anne Franks, han participado de este debate. ACLU no sólo ha brindado testimonio público sino que ha iniciado un litigio contra el Estado de Arizona por haber aprobado una ley "extensiva, basada en el contenido que criminaliza la exhibición, publicación y venta de imágenes no –obscenas, protegidas por la primera Enmienda–".[95] También exigió que la ley se limite a supuestos en los que exista una intención de dañar y una relación íntima entre la víctima y el autor del contenido.

Franks, por su parte, ha respondido con furia a este reclamo de ACLU, argumentando que:

---

93 Jeong, Sarah, "*Revenge Porn is bad. Criminalizing it is* worse", en; Wired, 28 de octubre de 2013, disponible en: http://bit.ly/1SVZU9B.

94 "Ante la importancia que asume la problemática de la discriminación, es interesante conocer cómo esperan las personas consultadas que actúe el Estado al respecto. El Gráfico Nº 1.10 muestra que en el 39% de las respuestas (51% de los/as entrevistadas/os) se señala que se deben realizar más campañas de difusión e información. Siendo que el 65% de las personas (38% de respuestas) entiende la discriminación como una falta de educación (Gráfico Nº 1.2), no sorprende que la mayor cantidad de personas opine que el Estado tenga que generar una mayor cantidad de espacios de instrucción y sensibilización a fin de combatir la discriminación. Por su parte, las siguientes tres respuestas con mayor cantidad de acuerdo por parte de la población encuestada hacen referencia a un tipo de actuación estatal que pone énfasis en lo punitivo, ya sea ampliando los lugares donde realizar denuncias, aplicando multas y/o sanciones o dictando nuevas leyes que penalicen los actos discriminatorios." INADI, *Mapa de la Discriminación 2013.* 30 de Octubre de 2013, p. 31, disponible en: http://bit.ly/1xrp2sV.

95 *Véase, http://bit.ly/1riJfgT.*

> No es sorprendente que un grupo de varones universitarios que tienen el hábito de circular imágenes de mujeres en estado de inconsciencia, desnudas, para su propio entretenimiento promuevan una definición estrecha e ilógica de este comportamiento criminal. Sin embargo, es profundamente decepcionante que una organización supuestamente dedicada a las libertades civiles haga lo mismo.[96]

La autora sostiene que las leyes de pornografía de venganza deben incluir a cualquier persona divulgando imágenes íntimas sin consentimiento y que la intención de dañar es irrelevante. No obstante, recomienda incluir una excepción de interés público.

En la presente investigación se adopta algo de las dos posturas. En caso de adherir el regulador a la opción de criminalización, esta solo debería abarcar a quien publica y pone a disposición el material, si tuvo una relación íntima con la víctima (no necesariamente una pareja estable). Por otra parte, la intención de dañar es irrelevante y la excepción de interés público dependerá del enfoque en que se sustente el delito. Si se funda en un supuesto de discurso de odio o de agresión sexual, no existiría ningún interés público a proteger. Si el delito se fundara en una violación a la privacidad, la libertad de expresión podría justificar una excepción de este tipo (por ejemplo, la participación de políticos en algún tipo de actividad sexual).

Debe considerarse especialmente que si bien la criminalización se adoptó tanto en sistemas jurídicos regulados por los sistemas de derechos humanos (Europa) como los que no (Estados Unidos, donde los pactos internacionales de derechos humanos no son superiores a la ley), la realidad es que en Estados Unidos, cuya legislación civil es más restrictiva al momento de conceder indemnizaciones y que no tiene el respaldo de los derechos humanos en relación con la privacidad o la violencia contra las mujeres, la criminalización sea una herramienta más eficaz. En Argentina, la vía procesal del artículo 43 de la Constitución Nacional mediante la acción de amparo o el hábeas data y la reparación de daños puede ser más eficaz que la persecución penal (que no ha detenido a ningún feminicida, o al menos no hay pruebas de ello). Sería importante analizar empíricamente, antes de crear el tipo penal, si la criminalización causa un efecto preventivo en casos de discurso de odio o de violación a la privacidad.

---

96 Franks, Mary Anne, "*The ACLU's Frat House Take on 'Revenge Porn*", en: Huffington Post, 4 de enero de 2015, disponible en: http://huff.to/1RYmApx. Traducción propia.

Como lo advirtió recientemente (noviembre de 2015) el Foro de Buenas Prácticas "Lucha contra la violencia en línea y el abuso de mujeres" del Internet Governance Forum:

> En aquellos países que estén considerando desarrollar respuestas legislativas a este problema, es importante que los remedios y compensaciones sean priorizadas por sobre la criminalización. No solo deben los gobiernos priorizar el acceso a la justicia de víctimas y sobrevivientes de abusos en línea y violencia de género sino que medidas flexibles e informales (pero transparentes) que puedan brindar una respuesta fácil, rápida y efectiva al comportamiento en línea deben ser investigadas con mayor profundidad.[97]

Convertir una conducta en delito penal tiene por supuesto, consecuencias gravosas para las libertades individuales. Pero además en este caso, en que la conducta implica publicar o poner a disposición contenido, la criminalización tiene un especial impacto en la libertad de expresión. Esto ya ha sido advertido por las relatorías especiales en sus declaraciones conjuntas y en el Informe Anual de la Relatoría Especial para la Libertad de Expresión de la CIDH (2013), en referencia a otros supuestos como difamación o *grooming*:"La difamación penal no es una restricción justificable de la libertad de expresión; debe derogarse la legislación penal sobre difamación y sustituirse, conforme sea necesario, por leyes civiles de difamación apropiadas".[98]

Como ya se dijo, no existe en principio, en el supuesto de pornografía no consentida, un interés público a resguardar si se lo califica como discurso de odio, por lo cual la restricción al discurso por medio de la amenaza de sanción penal aparece como legítima. Distinto es el caso de la afectación de la privacidad.[99] Por supuesto, siempre y cuando el tipo penal esté bien delimitado y no se haga extensivo a otros sujetos que no son los autores de la publicación o

---

97 IGF, Documento borrador aún no publicado. Traducción propia.

98 CIDH, y otros, *Declaración conjunta sobre libertad de expresión y administración de justicia, Comercialización y libertad de expresión, y difamación penal,* 2002, disponible en: http://bit.ly/1TAh8Zt.

99 "La protección de la honra y la reputación, cuando se alega una afectación mediante el uso de internet, debe responder en general a criterios de ponderación similares a los que se utilizan en otros ámbitos de la comunicación. En particular, como lo ha sostenido de manera reiterada la CIDH, resulta desproporcionada la aplicación del derecho penal cuando se trata de discursos especialmente protegidos, esto es, informaciones o expresiones sobre asuntos de interés público, funcionarios públicos o personas voluntariamente comprometidas en asuntos de interés público". CIDH, *Informe Anual 2009. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión)*, OEA/Ser.L/V/II. Doc. 51, párrafos. 101 y ss.

puesta a disposición o no se contemplen otras situaciones distintas al material sexual explícito.

En este sentido, la Declaración Conjunta sobre Libertad de Expresión y la respuesta a situaciones de conflicto (2015) advierte que:

> Todas las restricciones criminales sobre el contenido –incluyendo aquellas relacionadas con el discurso de odio, seguridad nacional, orden público, y terrorismo/extremismo– deberían conformarse estrictamente bajo los estándares internacionales, lo que incluye no proporcionar una protección especial a funcionarios y no emplear términos vagos o indebidamente amplios.[100]

Ahora bien, la criminalización no modifica la cuestión de la remoción del material de donde sea que esté publicado, la cual sigue rigiéndose por los parámetros de libertad de expresión del Sistema Interamericano. Sólo modifica la sanción al autor y eventualmente, la prevención, si es que la criminalización efectivamente actuara como un elemento disuasivo.

En relación con los intermediarios de internet, estos deberían quedar fuera de todo tipo de sanción criminal (sobre la responsabilidad civil, el estándar es de negligencia luego de notificación de la ilegitimidad del material por una judicial o de autoridad administrativa competente) ya que sólo se limitan a servir de herramienta para la acción del autor/agresor. Igualmente, es destacable que la gran mayoría de los intermediarios, comprendiendo la gravedad de la problemática, se autorreguló e incluyó en sus términos y condiciones los mecanismos para que las víctimas soliciten la remoción del material comprometiéndose a una remoción inmediata.[101] Es para celebrar que los intermediarios puedan adaptar sus propios estándares a los estándares de derechos humanos.[102]

Vale decir que la autorregulación ha sido propuesta por la RELE como un estándar a ser promovido como una alternativa a la criminalización, a fin de resguardar la libertad de expresión: "La autorregulación puede ser una

---

100 CIDH y otros, *Declaración Conjunta sobre Libertad de Expresión y la respuesta a situaciones de conflicto,* 2015, disponible en: http://bit.ly/1maIjwB.

101 *Véase*, Cyber Civil Rights Initiative, "Online Removal Guide", disponible en: http://bit.ly/1jR-QT2R. *Véase también,* Declaración de prensa de Pornhub, del 13 de Octubre de 2015, en la que se compromete a remover cualquier material que la victima indique como privado y publicado sin su consentimiento, disponible en: http://bit.ly/1Q9Z6I3.

102 *Véase,* IGF, Best Practice Forum, "*Countering Online Violence Against and Abuse of Women*. 2015, documento borrador no publicado.

herramienta efectiva para abordar las expresiones injuriosas y, por lo tanto, debe ser promovida."[103]

Varios artículos especializados se han hecho eco de las modificaciones en las políticas de las empresas y han destacado que esta es una medida mucho más simple y eficiente que aprobar leyes. Para el ciudadano, observan, es mejor que la empresa se autoregule a que el gobierno les diga que pueden o no decir en línea. [104]

Asimismo, en algunos casos que pueden llegar a ser muy eficaces, el Estado se ha asociado a las empresas que prestan servicios de intermediación en internet para combatir la "ciberexplotación". Este es el caso del "Cyber Exploitation", una iniciativa lanzada por la Procuradora General de California en conjunto con las principales empresas de internet.[105] Esta página sistematiza recursos como por ejemplo los enlaces de las empresas para solicitar la remoción de contenido por pornografía de venganza (en un mismo lugar, así la víctima no debe buscar uno por uno) y también una guía de buenas prácticas. Esta clase de iniciativas son medidas que pueden ser tanto o más eficaces que la criminalización.

Finalmente, debe analizarse que la criminalización de la pornografía no consentida podría autorizar, eventualmente, la requisa del material prohibido, tanto al Intermediario como al autor/agresor. En relación con el presunto autor, autorizaría el análisis de sus herramientas de comunicación y en relación con el intermediario podría ocasionar trastornos en la prestación del servicio a todos los demás usuarios. Este es otro factor para considerar la proporcionalidad de criminalizar esta acción.

V. Conclusión

Como conclusión, se pone de resalto que la pornografía no consentida es un problema global que merece atención regulatoria. Los sistemas de derechos humanos ofrecen alternativas para encuadrar este fenómeno discursivo (se trata de contenido), tales como el discurso de odio, –por tratarse de un caso de violencia contra las mujeres–, o, el derecho a la privacidad que también

103 CIDH y otros, *Declaración Conjunta sobre Libertad de Expresión e internet,* disponible en: http://bit.ly/1fgvszj

104 Daileda, Colin, "*Social Media sites may be better than the law at blocking revenge porn*", en: Mashable, 18 de marzo de 2015, disponible en: http://on.mash.to/1PSySzL.

105 *Véase,* Office of the Attorney General, "Cyberexplotaition", disponible en: http://bit.ly/23H-b2Lq.

brinda suficiente protección. De forma paralela, las leyes domésticas deben permitir la procedencia de indemnizaciones por los daños y perjuicios ocasionados y un rápido acceso a la justicia para las víctimas.

El encuadre como discurso de odio permite una protección más eficaz, ya que el Sistema Interamericano permite su prohibición y ello excluye la existencia de interés público a balancear; mientras el derecho a la privacidad exige que la restricción del contenido se confronte con un eventual interés público en la circulación del contenido.

El derecho penal también se presenta como una alternativa, y ha sido receptada por muchos países que consideran a la criminalización como la única herramienta realmente disuasiva. Se advierte, no obstante, que previo al abordaje penal, el Estado debe construir estadísticas que avalen acudir a la criminalización, que debe ser siempre la última ratio regulatoria.

En cualquiera de los escenarios, el Estado debería garantizar el rápido y fácil acceso a la justicia para las víctimas adoptando o creando los mecanismos procesales más aptos para una rápida solución del problema de la circulación del contenido.

Por otra parte, de acuerdo con los estándares de la RELE, los derechos de los intermediarios de internet deben ser resguardados de toda sanción, excepto casos de negligencia ante una orden judicial o de autoridad administrativa que ordene remover el contenido, como medida de responsabilidad ulterior decretada contra el autor del contenido.

Por último se destaca que cualquier opción regulatoria debe partir de una definición clara del problema que se pretende regular. Es decir, deben definirse los contornos del objeto a regular con suma claridad. Ello evitará la adopción de políticas erróneas que no solo no protejan a las víctimas sino que además podrían vulnerar otros derechos fundamentales.

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) fue creado en el año 2009 dentro del ámbito de la Facultad de Derecho de la Universidad de Palermo con el objetivo de realizar estudios e investigaciones que se constituyan en herramientas útiles para periodistas, instituciones gubernamentales, sectores privados y de la sociedad civil dedicados a la defensa y promoción de estos derechos, especialmente en América Latina.

La creación del CELE responde a la necesidad de construir espacios de debate dedicados a reflexionar sobre la importancia, los contenidos y los límites de estos derechos en la región. Para esto, el centro se propone dialogar y trabajar en conjunto con otras unidades académicas del país y de América Latina.

En este marco, los objetivos específicos del CELE son:

- Desarrollar estudios y guías de recomendaciones que tengan impacto en las políticas públicas vinculadas con el acceso a la información y a la libertad de expresión.
- Fomentar junto con distintas unidades académicas la profundización de estudios en cuestiones vinculadas con estos derechos.
- Contribuir a la generación de conciencia sobre la importancia de estos derechos en sociedades democráticas, fundamentalmente en las nuevas generaciones.







Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información
Mario Bravo 1050, 7o P (C1175ABT), Buenos Aires. Tel.: (54 11) 5199-4500 int. 1213
www.palermo.edu/cele